JC03 Rec'd PCT/PTO 24 JUL 2001

FORM PTO-1390
(REV 10-94)

U S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER
9320.134USWO

U S APPLICATION NO (If known, see 37 C F R 1 5)
Unknown 09/889918

INTERNATIONAL APPLICATION NO	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/FR00/00190	January 27, 2000	January 27, 1999

TITLE OF INVENTION

METHOD FOR PROVING THE AUTHENTICITY OF AN ENTITY AND/OR THE INTEGRITY OF A MESSAGE BY MEANS OF A PUBLIC EXPONENT EQUAL TO THE POWER OF TWO

APPLICANT(S) FOR DO/EO/US

GUILLOU et al.

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. [X] This is a **FIRST** submission of items concerning a filing under 35 U.S C. 371.
2. [ ] This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. [X] This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. [X] A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. [X] A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. [X] is transmitted herewith (required only if not transmitted by the International Bureau).
   b. [X] has been transmitted by the International Bureau.
   c. [ ] is not required, as the application was filed in the United States Receiving Office (RO/US)
6. [X] A translation of the International Application into English (35 U S C 371(c)(2))
7. [X] Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. [ ] are transmitted herewith (required only if not transmitted by the International Bureau)
   b. [ ] have been transmitted by the International Bureau.
   c. [ ] have not been made; however, the time limit for making such amendments has NOT expired
   d. [X] have not been made and will not be made.
8. [ ] A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. [X] An oath or declaration of the inventor(s) (35 U S.C. 371 (c)(4)).
10. [X] A translation of the annexes to the International Preliminary Examination Report under PCT Article 34 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern document(s) or information included:

11. [ ] An Information Disclosure Statement under 37 CFR 1.97 and 1 98.
12. [ ] An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. [X] A FIRST preliminary amendment.
    [ ] A SECOND of SUBSEQUENT preliminary amendment
14. [ ] A substitute specification.
15. [ ] A change of power of attorney and/or address letter
16. [X] Other items or information: International Preliminary Examination Report and translation; International Search Report; Front page of PCT application

JC17 Rec'd PCT/PTO 24 JUL 2001

U.S. APPLICATION NO (If known, see 37 C F R 1 5)	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
Unknown 09/889918	PCT/FR00/00190	9320.134USWO

17. [X] The following fees are submitted:

	CALCULATIONS	PTO USE ONLY
BASIC NATIONAL FEE (37 CFR 1.492(a) (1)-(5)): Search Report has been prepared by the EPO or JPO .... **$860.00** International preliminary examination fee paid to USPTO (37 CFR 1.492(a)(1)) .... **$690.00** No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2)) .... **$710.00** Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1 445(a)(3)) paid to USPTO .... **$1000.00** International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) **$100.00**		
ENTER APPROPRIATE BASIC FEE AMOUNT =	**$860.00**	
Surcharge of **$130.00** for furnishing the oath or declaration later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1.492(e))	**$0**	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	16 -20 =	0	X **$18.00**	**$0**	
Independent claims	4 -3 =	1	X **$80.00**	**$80.00**	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ **$260.00**	**$0**	
TOTAL OF ABOVE CALCULATIONS =				**$940.00**	
Reduction by 1/2 for filing by small entity, if applicable. Small entity status is claimed pursuant to 37 CFR 1.27				**$0**	
SUBTOTAL =				**$940.00**	
Processing fee of **$130.00** for furnishing the English translation later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1 492(f). +				**$0**	
TOTAL NATIONAL FEE =				**$940.00**	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3 28, 3.31). $40.00 per property +				**$0**	
TOTAL FEES ENCLOSED =				**$940.00**	
				Amount to be: refunded	**$0**
				charged	**$0**

a. [X] Check in the amount of $940.00 to cover the above fees is enclosed.

b. [ ] Please charge my Deposit Account No ________________ in the amount of $ ____________ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. [X] The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No 13-2725.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO
John J. Gresens
MERCHANT & GOULD
P.O. Box 2903
Minneapolis, MN 55402-0903

SIGNATURE: [signature]

NAME: John J. Gresens

REGISTRATION NUMBER: 33,112

09/889918
JC17 Rec'd PCT/PTO 24 JUL 2001

S/N unknown

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	GUILLOU et al.	Docket No.:	9320.134USWO
Serial No.:	unknown	Filed:	concurrent herewith
Int'l Appln No.:	PCT/FR00/00190	Int'l Filing Date:	January 27, 2000
Title:	METHOD FOR PROVING THE AUTHENTICITY OF AN ENTITY.....		

CERTIFICATE UNDER 37 CFR 1.10
'Express Mail' mailing label number: EL669941910US
Date of Deposit: July 24, 2001
I hereby certify that this correspondence is being deposited with the United States Postal Service 'Express Mail Post Office To Addressee' service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington, D C. 20231.
By:
Name: Omesh Singh

PRELIMINARY AMENDMENT

Box PCT
Assistant Commissioner for Patents
Washington, D. C. 20231

Dear Sir:

In connection with the above-identified application filed herewith, please enter the following preliminary amendment, which is based on the Article 34 amendments, based on claims amended in prosecution of the international application and published in the International Preliminary Examination Report, a copy of which is enclosed herewith (marked-up copy attached):

IN THE ABSTRACT

Insert the attached Abstract page into the application as the last page thereof.

IN THE SPECIFICATION

A courtesy copy of the present specification is enclosed herewith. However, the World Intellectual Property Office (WIPO) copy should be relied upon if it is already in the U.S. Patent Office.

IN THE CLAIMS

Please amend the following claims:

7. (Amended) A system according to claim 6, designed to prove the authenticity of an entity called a demonstrator and an entity called a controller,
said system being such that it comprises:

- a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

- a controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device;

said system enabling the execution of the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, **m** being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $p_1, p_2, \ldots p_f$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \cdot Q_i^v \equiv 1 \ . \bmod n \text{ or } G_i \equiv Q_i^v \bmod n;$$

v designating a public exponent such that

$$v = 2^k$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \dots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$\mathbf{x^2 \equiv g_i \bmod n} \quad \text{and} \quad \mathbf{x^2 \equiv - g_i \bmod n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$\mathbf{x^v \equiv g_i^2 \bmod n}$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors $\mathbf{p_i}$ and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values $\mathbf{Q_i}$ and/or the **f.m** components $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j} \equiv Q_i \bmod p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v \bmod n}$$

where **r** is a random value such that $\mathbf{0 < r < n}$,

• or

• • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^v \bmod p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\mathbf{\{r_1, r_2, \dots r_f\}}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers $\mathbf{d_i}$ hereinafter called elementary challenges; the witness, on the basis of each challenge **d,** computes a response **D,**

• either by performing operations of the type:

$$\mathbf{D \equiv r \,.\, Q_1^{d1} \,.\, Q_2^{d2} \,.\, \dots \, Q_m^{dm} \bmod n}$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}{}^{d1} \cdot Q_{i,2}{}^{d2} \cdot \ldots Q_{i,m}{}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** process specified according to claim 1,

where as the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

the demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator, to transmit all or part of each commitment **R** to the controller device through the connection means;

• **Step 2: act of challenge d**

the controller device comprises challenge production means for the production, after receiving all or part of each commitment **R**, of the challenges **d** equal in number to the number of commitments **R,**

the controller device also has transmission means, hereinafter known as the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means.

• **Step 3: act of response D**

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the demonstrator device through the interconnection means,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, **m** being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $p_1, p_2, \ldots p_f$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \cdot Q_i^v \equiv 1 \,.\, \bmod n \text{ or } G_i \equiv Q_i^v \bmod n;$$

v designating a public exponent such that

$$v = 2^k$$

where **k** is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the **f** prime factors $p_1, p_2, \dots p_f$; the base number g_i being such that the following two conditions are met: neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv - g_i \bmod n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or the **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent **v**;

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where **r** is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \dots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d**, computes a response **D**,

• either by performing operations of the type:

$$D \equiv r \,.\, Q_1^{\,d1} \,.\, Q_2^{\,d2} \,.\, \ldots\, Q_m^{\,dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \,.\, Q_{i,1}^{\,d1} \,.\, Q_{i,2}^{\,d2} \,.\, \ldots\, Q_{i,m}^{\,dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** process specified according to claim 1,

• **Step 4: act of checking**

the transmission means of the demonstrator transmit each response **D** to the controller,

the controller device also comprises:

- computation means, hereinafter called the computation means of the controller device,
- comparison means, hereinafter called the comparison means of the controller device,

case where the demonstrator has transmitted a part of each commitment R.

if the transmission means of the demonstrator have transmitted a part of each commitment **R**, the computation means of the controller device, having **m** public values $G_1, G_2, \ldots, G_m$, compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$R' \equiv G_1^{\,d1} \,.\, G_2^{\,d2} \,.\, \ldots\, G_m^{\,dm} \,.\, D^v \bmod n$$

or a relationship of the type

$$R' \equiv D^v / G_1^{\,d1} \,.\, G_2^{\,d2} \,.\, \ldots\, G_m^{\,dm} \,.\, \bmod n$$

the comparison means of the controller device compare each reconstructed commitment **R'** with all or part of each commitment **R** received,

case where the demonstrator has transmitted the totality of each commitment R

if the transmission means of the demonstrator have transmitted the totality of each commitment **R**, the computation means and the comparison means of the controller device, having **m** public values $G_1, G_2, \ldots, G_m$, ascertain that each commitment **R** satisfies a relationship of the type

$$R \equiv G_1^{\,d1} \,.\, G_2^{\,d2} \,.\, \ldots\, G_m^{\,dm} \,.\, D^v \bmod n$$

or a relationship of the type

$$R \equiv D^{v}/G_1^{\ d1} \,.\, G_2^{\ d2} \,. \ldots G_m^{\ dm} \,.\, \mathrm{mod}\ n$$

8. (Amended) System according to claim 6, designed to give proof to an entity, known as a controller, of the integrity of a message **M** associated with an entity known as a demonstrator, said system being such that it comprises

- a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

- a controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device;

said system enabling the execution of the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, m being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $p_1, p_2, \ldots p_f$, f being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \,.\, Q_i^{\ v} \equiv 1 \,.\, \mathrm{mod}\ n \text{ or } G_i \equiv Q_i^{\ v} \ \mathrm{mod}\ n;$$

v designating a public exponent such that

$$v = 2^{k}$$

where **k** is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the **f** prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met: neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv - g_i \bmod n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n**;

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or the **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent **v**;

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where **r** is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d**, computes a response **D**,

• either by performing operations of the type:

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

• or

• • by performing operations of the type:

$$\mathbf{D_i \equiv r_i \cdot Q_{i,1}{}^{d1} \cdot Q_{i,2}{}^{d2} \cdot \ldots\ Q_{i,m}{}^{dm} \bmod p_i}$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** process specified in claim 1,

where as the witness device has transmission means, hereinafter called transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

• **Step 2: act of challenge d**

the demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute at least one token **T,**

the demonstrator device also has transmission means, hereinafter known as the transmission means of the demonstrator device, to transmit each token **T** through the connection means to the controller device,

the controller device also has challenge production means for the production, after having received the token **T**, of the challenges **d** in a number equal to the number of commitments **R**,

the controller device also has transmission means, hereinafter called the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means;

• **Step 3: act of response D**

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the demonstrator device through the interconnection means,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \cdot Q_i^v \equiv 1 \,.\, \mathrm{mod}\ n \text{ or } G_i \equiv Q_i^v \bmod n;$$

v designating a public exponent such that

$$v = 2^k$$

where **k** is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the **f** prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met: neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv -\, g_i \bmod n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or the **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where **r** is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i

hereinafter called elementary challenges; the witness, on the basis of each challenge **d,** computes a response **D**,

• either by performing operations of the type:

$$\mathbf{D \equiv r \,.\, Q_1{}^{d1} \,.\, Q_2{}^{d2} \ldots\, Q_m{}^{dm} \bmod n}$$

• or

• • by performing operations of the type:

$$\mathbf{D_i \equiv r_i \,.\, Q_{i,1}{}^{d1} \,.\, Q_{i,2}{}^{d2} \ldots\, Q_{i,m}{}^{dm} \bmod p_i}$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** process specified according to claim 1,

• **Step 4: act of checking**

the transmission means of the demonstrator transmit each response **D** to the controller,

the controller device also comprises computation means, hereinafter called the computation means of the controller device, having **m** public values $\mathbf{G_1, G_2, \ldots, G_m}$, to firstly compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$\mathbf{R' \equiv G_1{}^{d1} \,.\, G_2{}^{d2} \,. \ldots\, G_m{}^{dm} \,.\, D^v \bmod n}$$

or a relationship of the type

$$\mathbf{R' \equiv D^v / G_1{}^{d1} \,.\, G_2{}^{d2} \,. \ldots\, G_m{}^{dm} \,.\, \bmod n}$$

then, secondly, compute a token **T'** by applying the hashing function **h** having as arguments the message **M** and all or part of each reconstructed commitment **R'**,

the controller device also has comparison means, hereinafter known as the comparison means of the controller device, to compare the computed token **T'** with the received token **T**.

9. (Amended) System according to claim 6, designed to produce the digital signatúre of a message **M**, hereinafter known as the signed message, by an entity called a signing entity;

the signed message comprising:

- the message **M,**

- the challenges **d** and/or the commitments **R,**

- the responses **D**;

Signing operation

said system being such that it comprises a signing device associated with the signing entity, said signing device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said system enabling the execution of the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \cdot Q_i^v \equiv 1 \,.\, mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^v\, mod\ n};$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$\mathbf{x^2 \equiv g_i\, mod\ n} \quad \text{and} \qquad \mathbf{x^2 \equiv -\, g_i\, mod\ n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$\mathbf{x^v \equiv g_i^2\, mod\ n}$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors $\mathbf{p_i}$ and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values $\mathbf{Q_i}$ and/or the **f.m** components $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j} \equiv Q_i \bmod p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v \bmod n}$$

where **r** is a random value such that $\mathbf{0 < r < n}$,

• or

• • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^{\,v} \bmod p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\mathbf{\{r_1, r_2, \ldots r_f\}}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers $\mathbf{d_i}$ hereinafter called elementary challenges; the witness, on the basis of each challenge **d,** computes a response **D**,

• either by performing operations of the type:

$$\mathbf{D \equiv r \,.\, Q_1^{\ d1} \,.\, Q_2^{\ d2} \,.\, \ldots\, Q_m^{\ dm} \bmod n}$$

• or

• • by performing operations of the type:

$$\mathbf{D_i \equiv r_i \,.\, Q_{i,1}^{\ d1} \,.\, Q_{i,2}^{\ d2} \,.\, \ldots\, Q_{i,m}^{\ dm} \bmod p_i}$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** process specified according to claim 1,

where as the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

• **Step 2: act of challenge d**

the signing device comprises computation means, hereinafter called the computation means of the signing device, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute a binary train and extract, from this binary train, challenges **d** whose number is equal to the number of commitments **R**,

• **Step 3: act of response D**

the means for the reception of the challenges **d** of the witness device receive each challenge **d** coming from the signing device through the interconnection means,

the means for computing the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \cdot Q_i^v \equiv 1 \,.\, mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^v\ mod\ n};$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$\mathbf{x^2 \equiv g_i\ mod\ n} \quad \text{and} \quad \mathbf{x^2 \equiv -\, g_i\ mod\ n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$\mathbf{x^v \equiv g_i^2\ mod\ n}$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors $\mathbf{p_i}$ and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values $\mathbf{Q_i}$ and/or the **f.m** components $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j} \equiv Q_i \bmod p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent **v**;

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v \bmod n}$$

where **r** is a random value such that $\mathbf{0 < r < n}$,

• or

• • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^v \bmod p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\{\mathbf{r_1}, \mathbf{r_2}, \ldots \mathbf{r_f}\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers $\mathbf{d_i}$ hereinafter called elementary challenges; the witness, on the basis of each challenge **d**, computes a response **D**,

• either by performing operations of the type:

$$\mathbf{D \equiv r \,.\, Q_1^{d1} \,.\, Q_2^{d2} \,.\, \ldots\, Q_m^{dm} \bmod n}$$

• or

• • by performing operations of the type:

$$\mathbf{D_i \equiv r_i \,.\, Q_{i,1}^{d1} \,.\, Q_{i,2}^{d2} \,.\, \ldots\, Q_{i,m}^{dm} \bmod p_i}$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** process specified according to claim 1,

where as the witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses **D** to the signing device through the interconnection means.

12. (Amended) A terminal device according to claim 11, designed to prove the authenticity of an entity called a demonstrator to an entity called a controller.

said terminal device being such that it comprises a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and being capable especially of taking the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said demonstrator device also comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

said terminal device enabling the execution of the following steps:

- **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \,.\, Q_i^v \equiv 1 \,.\, mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^v\ mod\ n};$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1,

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met: neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv - g_i \bmod n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or the **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where **r** is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d,** computes a response **D,**

• either by performing operations of the type:

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** process specified according to claim 1,

where as the witness device has transmission means, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

the demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator, to transmit all or part of each commitment **R** to the controller device, through the connection means;

- **Steps 2 and 3: act of challenge d, act of response D**

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the controller device through the connection means between the controller device and the demonstrator device and through the interconnection means between the demonstrator device and the witness device,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i . Q_i^v \equiv 1 . \bmod n} \text{ or } \mathbf{G_i \equiv Q_i^v \bmod n};$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv - g_i \bmod n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or the **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where **r** is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d,** computes a response **D,**

• either by performing operations of the type:

$$D \equiv r \,.\, Q_1^{d1} \,.\, Q_2^{d2} \,.\, \ldots\, Q_m^{dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \,.\, Q_{i,1}^{d1} \,.\, Q_{i,2}^{d2} \,.\, \ldots\, Q_{i,m}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** process specified according to claim 1,

• **Step 4: act of checking**

the transmission means of the demonstrator transmit each response **D** to the controller that carries out the check.

13. (Amended) Terminal device according to claim 11, designed to give proof to an entity, known as a controller, of the integrity of a message **M** associated with an entity known as a demonstrator,

said terminal device being such that it comprises a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and being capable especially of taking the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said demonstrator device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

said terminal device being used to execute the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1}$, $\mathbf{Q_2}$, ... $\mathbf{Q_m}$ and public values $\mathbf{G_1}$, $\mathbf{G_2}$, ... $\mathbf{G_m}$, **m** being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1}$, $\mathbf{p_2}$, ... $\mathbf{p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \cdot Q_i^v \equiv 1 \cdot mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^v\ mod\ n;}$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$\mathbf{x^2 \equiv g_i\ mod\ n} \quad \text{and} \quad \mathbf{x^2 \equiv -\ g_i\ mod\ n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$\mathbf{x^v \equiv g_i^2\ mod\ n}$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors $\mathbf{p_i}$ and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values $\mathbf{Q_i}$ and/or the **f.m** components $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j} \equiv Q_i\ mod\ p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v\ mod\ n}$$

where **r** is a random value such that $\mathbf{0 < r < n}$,

• or

• • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^v\ mod\ p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\mathbf{\{r_1, r_2, \ldots r_f\}}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers $\mathbf{d_i}$ hereinafter called elementary challenges; the witness, on the basis of each challenge **d,** computes a response **D**,

• either by performing operations of the type:

$$\mathbf{D \equiv r \cdot Q_1^{\ d1} \cdot Q_2^{\ d2} \cdot \ldots Q_m^{\ dm} \bmod n}$$

• or

• • by performing operations of the type:

$$\mathbf{D_i \equiv r_i \cdot Q_{i,1}^{\ d1} \cdot Q_{i,2}^{\ d2} \cdot \ldots Q_{i,m}^{\ dm} \bmod p_i}$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** process specified according to claim 1;

where as the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

• Steps 2 and 3: act of challenge d, act of response D

the demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute at least one token **T,**

the demonstrator device also has transmission means, hereinafter known as the transmission means of the demonstrator device, to transmit each token **T,** through the connection means, to the controller device,

said controller, after having received the token **T**, produces challenges **d** equal in number to the number of commitments **R,**

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the controller device through the connection means between the controller device and the demonstrator device and through the interconnection means between the demonstrator device and the witness device,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m, m}$

being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $p_1, p_2, \ldots p_f$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \cdot Q_i^v \equiv 1 \,.\, \text{mod } n \text{ or } G_i \equiv Q_i^v \text{ mod } n;$$

v designating a public exponent such that

$$v = 2^k$$

where **k** is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the **f** prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \text{ mod } n \quad \text{and} \quad x^2 \equiv - g_i \text{ mod } n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \text{ mod } n$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or the **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \text{ mod } p_j$) of the private values Q_i and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \text{ mod } n$$

where **r** is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \text{ mod } p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i

belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d,** computes a response **D**,

• either by performing operations of the type:

$$D \equiv r \,.\, Q_1^{\,d1} \,.\, Q_2^{\,d2} \ldots Q_m^{\,dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \,.\, Q_{i,1}^{\,d1} \,.\, Q_{i,2}^{\,d2} \ldots Q_{i,m}^{\,dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** process specified according to claim 1,

• **Step 4: act of checking**

the transmission means of the demonstrator send each response **D** to the controller device which performs the check.

14. (Amended) Terminal device according to claim 11, designed to produce the digital signature of a message **M**, hereinafter known as the signed message, by an entity called a signing entity;

the signed message comprising:

- the message **M,**
- the challenges **d** and/or the commitments **R,**
- the responses **D**;

said terminal device being such that it comprises a signing device associated with the signing entity, said signing device being interconnected with the witness device by interconnection means and possibly taking especially the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said demonstrator device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

Signing operation

said terminal device being used to execute the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, **m** being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $p_1, p_2, \ldots p_f$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \cdot Q_i^v \equiv 1 \cdot \bmod n \text{ or } G_i \equiv Q_i^v \bmod n;$$

v designating a public exponent such that

$$v = 2^k$$

where **k** is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the **f** prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv - g_i \bmod n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors

$\mathbf{p_i}$ and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values $\mathbf{Q_i}$ and/or the **f.m** components $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j} \equiv Q_i \bmod p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent **v**;

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v \bmod n}$$

where **r** is a random value such that $\mathbf{0 < r < n}$,

• or

• • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^{\,v} \bmod p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\mathbf{\{r_1, r_2, \ldots r_f\}}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers $\mathbf{d_i}$ hereinafter called elementary challenges; the witness, on the basis of each challenge **d,** computes a response **D**,

• either by performing operations of the type:

$$\mathbf{D \equiv r \,.\, Q_1^{\,d1} \,.\, Q_2^{\,d2} . \ldots Q_m^{\,dm} \bmod n}$$

• or

• • by performing operations of the type:

$$\mathbf{D_i \equiv r_i \,.\, Q_{i,1}^{\,d1} \,.\, Q_{i,2}^{\,d2} . \ldots Q_{i,m}^{\,dm} \bmod p_i}$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** process specified according to claim 1,

where as the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the signing device through the interconnection means,

• **Step 2: act of challenge d**

the signing device comprises computation means, hereinafter called the computation means of the signing device, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute a binary train and extract, from this binary train, challenges **d** whose number is equal to the number of commitments **R**,

- **Step 3: act of response D**

the means for the reception of the challenges **d** of the witness device receive each challenge **d** coming from the signing device through the interconnection means,

the means for computing the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \cdot Q_i^v \equiv 1 \;.\; mod\; n} \text{ or } \mathbf{G_i \equiv Q_i^v\; mod\; n};$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$\mathbf{x^2 \equiv g_i\; mod\; n} \quad \text{and} \quad \mathbf{x^2 \equiv -\, g_i\; mod\; n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$\mathbf{x^v \equiv g_i^2\; mod\; n}$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors

$\mathbf{p_i}$ and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values $\mathbf{Q_i}$ and/or the **f.m** components $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j}} \equiv \mathbf{Q_i}$ **mod** $\mathbf{p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent **v**;

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v \bmod n}$$

where **r** is a random value such that $\mathbf{0 < r < n}$,

• or

• • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^v \bmod p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\{\mathbf{r_1}, \mathbf{r_2}, \ldots \mathbf{r_f}\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers $\mathbf{d_i}$ hereinafter called elementary challenges; the witness, on the basis of each challenge **d,** computes a response **D**,

• either by performing operations of the type:

$$\mathbf{D \equiv r \,.\, Q_1^{\,d1} \,.\, Q_2^{\,d2} . \ldots Q_m^{\,dm} \bmod n}$$

• or

• • by performing operations of the type:

$$\mathbf{D_i \equiv r_i \,.\, Q_{i,1}^{\,d1} \,.\, Q_{i,2}^{\,d2} . \ldots Q_{i,m}^{\,dm} \bmod p_i}$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** process specified according to claim 1,

where as the witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses **D** to the signing device, through the interconnection means.

<u>REMARKS</u>

The above preliminary amendment is made to remove multiple dependencies from claims 7, 8, 9, 12, 13 and 14.

A new abstract page is supplied to conform to that appearing on the publication page of the WIPO application, but the new Abstract is typed on a separate page as required by U.S. practice.

Applicants respectfully request that the preliminary amendment described herein be entered into the record prior to calculation of the filing fee and prior to examination and consideration of the above-identified application.

If a telephone conference would be helpful in resolving any issues concerning this communication, please contact Applicants' primary attorney-of record, John J. Gresens (Reg. No. 33,112), at (612) 371.5265.

Respectfully submitted,

MERCHANT & GOULD P.C.
P.O. Box 2903
Minneapolis, Minnesota 55402-0903
(612) 332-5300

Dated: <u>July 24, 2001</u>

By ____________________
John J. Gresens
Reg. No. 33,112

JJG/tvm

ABSTRACT

Title: METHOD FOR PROVING THE AUTHENTICITY OR INTEGRITY OF A MESSAGE BY MEANS OF A PUBLIC EXPONENT EQUAL TO THE POWER OF TWO

Proof is established by means of the following parameters: m pairs of private values Q_i and public values G_i m>1, a public module n made of the product of f first factors p_j, f>2, a public exponent v, linked to each other by relations of the type: $G_i.Q_i^v = 1 \bmod n$ or $G_i = Q_i^v \bmod n$. Said exponent v is such that $v=2^k$ where k>1 is a security parameter. Public value G_i is the square g_i^2 of a base number g_i that is lower than f first factors p_j, so that the two equations: $x2=g_i \bmod n$ and $x^2= -g_i \bmod n$ do not have a solution in x in the ring of the modulo n integers and such that the equation $x^v=g_i^2 \bmod n$ has solutions in x in the ring of the modulus n integers.

MARKED-UP COPY

7. (Amended) A system according to claim 6, designed to prove the authenticity of an entity called a demonstrator and an entity called a controller,

said system being such that it comprises:

- a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

- a controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device;

said system enabling the execution of the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \,.\, Q_i^v \equiv 1 \,.\, mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^v\ mod\ n;}$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv - g_i \bmod n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n**;

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or the **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent **v**;

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where **r** is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d**, computes a response **D**,

• either by performing operations of the type:

$$D \equiv r \,.\, Q_1^{d1} \,.\, Q_2^{d2} \,. \ldots\, Q_m^{dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \,.\, Q_{i,1}^{d1} \,.\, Q_{i,2}^{d2} \,. \ldots\, Q_{i,m}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** [process specified according to claim 1],

where as the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

the demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator, to transmit all or part of each commitment **R** to the controller device through the connection means;

- **Step 2: act of challenge d**

the controller device comprises challenge production means for the production, after receiving all or part of each commitment **R**, of the challenges **d** equal in number to the number of commitments **R**,

the controller device also has transmission means, hereinafter known as the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means.

- **Step 3: act of response D**

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the demonstrator device through the interconnection means,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \cdot Q_i^v \equiv 1 \,.\, mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^v\ mod\ n};$$

v designating a public exponent such that

$$v = 2^k$$

where **k** is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the **f** prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \qquad x^2 \equiv - g_i \bmod n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or the **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where **r** is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d**, computes a response **D**,

• either by performing operations of the type:

$$D \equiv r \,.\, Q_1^{d1} \,.\, Q_2^{d2} \,.\, \ldots\, Q_m^{dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \,.\, Q_{i,1}{}^{d1} \,.\, Q_{i,2}{}^{d2} \,.\, \ldots\, Q_{i,m}{}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced {**R, d, D**} [process specified according to claim 1],

• **Step 4: act of checking**

the transmission means of the demonstrator transmit each response **D** to the controller,

the controller device also comprises:

- computation means, hereinafter called the computation means of the controller device,
- comparison means, hereinafter called the comparison means of the controller device,

case where the demonstrator has transmitted a part of each commitment R.

if the transmission means of the demonstrator have transmitted a part of each commitment **R**, the computation means of the controller device, having **m** public values $G_1, G_2, \ldots, G_m$, compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$R' \equiv G_1{}^{d1} \,.\, G_2{}^{d2} \,.\, \ldots\, G_m{}^{dm} \,.\, D^v \bmod n$$

or a relationship of the type

$$R' \equiv D^v / G_1{}^{d1} \,.\, G_2{}^{d2} \,.\, \ldots\, G_m{}^{dm} \,.\, \bmod n$$

the comparison means of the controller device compare each reconstructed commitment **R'** with all or part of each commitment **R** received,

case where the demonstrator has transmitted the totality of each commitment R

if the transmission means of the demonstrator have transmitted the totality of each commitment **R**, the computation means and the comparison means of the controller device, having **m** public values $G_1, G_2, \ldots, G_m$, ascertain that each commitment **R** satisfies a relationship of the type

$$R \equiv G_1{}^{d1} \,.\, G_2{}^{d2} \,.\, \ldots\, G_m{}^{dm} \,.\, D^v \bmod n$$

or a relationship of the type

$$R \equiv D^v / G_1{}^{d1} \,.\, G_2{}^{d2} \,.\, \ldots\, G_m{}^{dm} \,.\, \bmod n$$

8. (Amended) System according to claim 6, designed to give proof to an entity, known as a controller, of the integrity of a message **M** associated with an entity known as a demonstrator, said system being such that it comprises

- a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

- a controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device;

said system enabling the execution of the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \cdot Q_i^v \equiv 1 \cdot mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^v\ mod\ n;}$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met: neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv - g_i \bmod n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or the **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where **r** is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d**, computes a response **D**,

• either by performing operations of the type:

$$D \equiv r \,.\, Q_1^{d1} \,.\, Q_2^{d2} \,.\, \ldots\, Q_m^{dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \,.\, Q_{i,1}^{d1} \,.\, Q_{i,2}^{d2} \,.\, \ldots\, Q_{i,m}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R**, **d**, **D** forming a triplet referenced {**R**, **d**, **D**} [process specified in claim 1],

where as the witness device has transmission means, hereinafter called transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

• **Step 2: act of challenge d**

the demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute at least one token **T**,

the demonstrator device also has transmission means, hereinafter known as the transmission means of the demonstrator device, to transmit each token **T** through the connection means to the controller device,

the controller device also has challenge production means for the production, after having received the token **T**, of the challenges **d** in a number equal to the number of commitments **R**,

the controller device also has transmission means, hereinafter called the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means;

• **Step 3: act of response D**

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the demonstrator device through the interconnection means,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \dots Q_m}$ and public values $\mathbf{G_1, G_2, \dots G_m}$, **m** being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \dots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i . Q_i^v \equiv 1 . \bmod n \text{ or } G_i \equiv Q_i^v \bmod n;$$

v designating a public exponent such that

$$v = 2^k$$

where **k** is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the **f** prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met: neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv - g_i \bmod n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or the **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where **r** is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d**, computes a response **D**,

• either by performing operations of the type:

$$D \equiv r \,.\, Q_1{}^{d1} \,.\, Q_2{}^{d2} \,.\, \ldots\, Q_m{}^{dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \,.\, Q_{i,1}{}^{d1} \,.\, Q_{i,2}{}^{d2} \,.\, \ldots\, Q_{i,m}{}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced {**R, d, D**} [process specified according to claim 1],

• **Step 4: act of checking**

the transmission means of the demonstrator transmit each response **D** to the controller,

the controller device also comprises computation means, hereinafter called the computation means of the controller device, having **m** public values $G_1, G_2, \ldots, G_m$, to firstly compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$R' \equiv G_1{}^{d1} \,.\, G_2{}^{d2} \,.\, \ldots\, G_m{}^{dm} \,.\, D^v \bmod n$$

or a relationship of the type

$$R' \equiv D^v / G_1{}^{d1} \,.\, G_2{}^{d2} \,.\, \ldots\, G_m{}^{dm} \,.\, \bmod n$$

then, secondly, compute a token **T'** by applying the hashing function **h** having as arguments the message **M** and all or part of each reconstructed commitment **R'**,

the controller device also has comparison means, hereinafter known as the comparison means of the controller device, to compare the computed token **T'** with the received token **T**.

9. (Amended) System according to claim 6, designed to produce the digital signature of a message **M**, hereinafter known as the signed message, by an entity called a signing entity;

the signed message comprising:

- the message **M**,
- the challenges **d** and/or the commitments **R**,
- the responses **D**;

Signing operation

said system being such that it comprises a signing device associated with the signing entity, said signing device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said system enabling the execution of the following steps:

- **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, m being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $p_1, p_2, \ldots p_f$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \,.\, Q_i^v \equiv 1 \,.\, \text{mod } n \text{ or } G_i \equiv Q_i^v \text{ mod } n;$$

v designating a public exponent such that

$$v = 2^k$$

where **k** is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the **f** prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \text{ mod } n \quad \text{and} \quad x^2 \equiv - g_i \text{ mod } n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \text{ mod } n$$

can be resolved in x in the ring of the integers modulo **n**;

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n**

and/or the **m** private values Q_i and/or the **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_i$) of the private values Q_i and of the public exponent **v**;

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where **r** is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d**, computes a response **D**,

• either by performing operations of the type:

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** [process specified according to claim 1],

where as the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

• **Step 2: act of challenge d**

the signing device comprises computation means, hereinafter called the computation means of the signing device, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute a binary train and extract, from this binary train, challenges **d** whose number is equal to the number of commitments **R**,

• **Step 3: act of response D**

the means for the reception of the challenges **d** of the witness device receive each challenge **d** coming from the signing device through the interconnection means,

the means for computing the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \cdot Q_i^v \equiv 1 \cdot mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^v\ mod\ n;}$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$\mathbf{x^2 \equiv g_i\ mod\ n} \quad \text{and} \quad \mathbf{x^2 \equiv -\ g_i\ mod\ n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$\mathbf{x^v \equiv g_i^2\ mod\ n}$$

can be resolved in x in the ring of the integers modulo **n**;

said method implements, in the following steps, an entity called a witness having **f** prime factors

$\mathbf{p_i}$ and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values $\mathbf{Q_i}$ and/or the **f.m** components $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j} \equiv Q_i \bmod p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

  • either by performing operations of the type:

$$\mathbf{R \equiv r^v \bmod n}$$

where **r** is a random value such that $\mathbf{0 < r < n}$,

  • or

    • • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^{\,v} \bmod p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\mathbf{\{r_1, r_2, \ldots r_f\}}$,

    • • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers $\mathbf{d_i}$ hereinafter called elementary challenges; the witness, on the basis of each challenge **d**, computes a response **D**,

  • either by performing operations of the type:

$$\mathbf{D \equiv r \,.\, Q_1^{\,d1} \,.\, Q_2^{\,d2} \,.\, \ldots\, Q_m^{\,dm} \bmod n}$$

  • or

    • • by performing operations of the type:

$$\mathbf{D_i \equiv r_i \,.\, Q_{i,1}^{\,d1} \,.\, Q_{i,2}^{\,d2} \,.\, \ldots\, Q_{i,m}^{\,dm} \bmod p_i}$$

    • • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** [process specified according to claim 1],

where as the witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses **D** to the signing device through the interconnection means.

12. (Amended) A terminal device according to claim 11, designed to prove the authenticity of an entity called a demonstrator to an entity called a controller.

said terminal device being such that it comprises a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and being capable especially of taking the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said demonstrator device also comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

said terminal device enabling the execution of the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, m being greater than or equal to 1 , or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $p_1, p_2, \ldots p_f$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \cdot Q_i^v \equiv 1 \, . \bmod n \text{ or } G_i \equiv Q_i^v \bmod n;$$

v designating a public exponent such that

$$v = 2^k$$

where **k** is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the **f** prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met: neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv -g_i \bmod n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^{v} \equiv g_i^{2} \bmod n$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or the **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^{v} \bmod n$$

where **r** is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^{v} \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d**, computes a response **D**,

• either by performing operations of the type:

$$D \equiv r \,.\, Q_1^{d1} \,.\, Q_2^{d2} \,.\, \ldots\, Q_m^{dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \,.\, Q_{i,1}^{d1} \,.\, Q_{i,2}^{d2} \,.\, \ldots\, Q_{i,m}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced {**R, d, D**} [process specified according to claim 1],

where as the witness device has transmission means, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

the demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator, to transmit all or part of each commitment **R** to the controller device, through the connection means;

• **Steps 2 and 3: act of challenge d, act of response D**

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the controller device through the connection means between the controller device and the demonstrator device and through the interconnection means between the demonstrator device and the witness device,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \,.\, Q_i^v \equiv 1 \,.\, mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^v\ mod\ n;}$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i}^2$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv - g_i \bmod n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or the **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where **r** is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d,** computes a response **D,**

• either by performing operations of the type:

$$D \equiv r \,.\, Q_1^{d1} \,.\, Q_2^{d2} \,.\, \ldots\, Q_m^{dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \,.\, Q_{i,1}^{d1} \,.\, Q_{i,2}^{d2} \,.\, \ldots\, Q_{i,m}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** [process specified according to claim 1],

• **Step 4: act of checking**

the transmission means of the demonstrator transmit each response **D** to the controller that carries out the check.

13. (Amended) Terminal device according to claim 11, designed to give proof to an entity, known as a controller, of the integrity of a message **M** associated with an entity known as a demonstrator,

said terminal device being such that it comprises a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and being capable especially of taking the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card, said demonstrator device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

said terminal device being used to execute the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i . Q_i^v \equiv 1 . \bmod n \text{ or } G_i \equiv Q_i^v \bmod n;$$

v designating a public exponent such that

$$v = 2^k$$

where **k** is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the **f** prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met: neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv - g_i \bmod n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or the **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where **r** is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d**, computes a response **D**,

• either by performing operations of the type:

$$D \equiv r \,.\, Q_1^{d1} \,.\, Q_2^{d2} \,.\, \ldots\, Q_m^{dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \,.\, Q_{i,1}^{d1} \,.\, Q_{i,2}^{d2} \,.\, \ldots\, Q_{i,m}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** [process specified according to claim 1];

where as the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

• Steps 2 and 3: act of challenge d, act of response D

the demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute at least one token **T**,

the demonstrator device also has transmission means, hereinafter known as the transmission means of the demonstrator device, to transmit each token **T**, through the connection means, to the controller device,

said controller, after having received the token **T**, produces challenges **d** equal in number to the number of commitments **R**,

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the controller device through the connection means between the controller device and the demonstrator device and through the interconnection means between the demonstrator device and the witness device,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m**

being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \dots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \cdot Q_i^v \equiv 1 \ . \bmod n} \text{ or } \mathbf{G_i \equiv Q_i^v \bmod n};$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \dots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$\mathbf{x^2 \equiv g_i \bmod n} \quad \text{and} \quad \mathbf{x^2 \equiv - g_i \bmod n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$\mathbf{x^v \equiv g_i^2 \bmod n}$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors $\mathbf{p_i}$ and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values $\mathbf{Q_i}$ and/or the **f.m** components $\mathbf{Q_{i,j}}$ $(\mathbf{Q_{i,j} \equiv Q_i \bmod p_j})$ of the private values $\mathbf{Q_i}$ and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v \bmod n}$$

where **r** is a random value such that $\mathbf{0 < r < n}$,

• or

• • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^v \bmod p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$

belonging to a collection of random values $\{r_1, r_2, \dots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d**, computes a response **D**,

• either by performing operations of the type:

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \dots Q_m^{dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \dots Q_{i,m}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** [process specified according to claim 1],

• **Step 4: act of checking**

the transmission means of the demonstrator send each response **D** to the controller device which performs the check.

14. (Amended) Terminal device according to claim 11, designed to produce the digital signature of a message **M**, hereinafter known as the signed message, by an entity called a signing entity;

the signed message comprising:

- the message **M**,
- the challenges **d** and/or the commitments **R**,
- the responses **D**;

said terminal device being such that it comprises a signing device associated with the signing entity, said signing device being interconnected with the witness device by interconnection means and possibly taking especially the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said demonstrator device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

Signing operation

said terminal device being used to execute the following steps:

- **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \cdot Q_i^v \equiv 1 \cdot mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^v\ mod\ n};$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$\mathbf{x^2 \equiv g_i\ mod\ n} \quad \text{and} \quad \mathbf{x^2 \equiv - g_i\ mod\ n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$\mathbf{x^v \equiv g_i^2\ mod\ n}$$

can be resolved in x in the ring of the integers modulo **n**;

said method implements, in the following steps, an entity called a witness having **f** prime factors

p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus $\mathbf{n}$ and/or the $\mathbf{m}$ private values $\mathbf{Q_i}$ and/or the $\mathbf{f.m}$ components $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j} \equiv Q_i \bmod p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent $\mathbf{v}$;

- the witness computes commitments $\mathbf{R}$ in the ring of the integers modulo $\mathbf{n}$; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v \bmod n}$$

where $\mathbf{r}$ is a random value such that $\mathbf{0 < r < n}$,

• or

• • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^v \bmod p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\{\mathbf{r_1, r_2, \ldots r_f}\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges $\mathbf{d}$, each challenge $\mathbf{d}$ comprising $\mathbf{m}$ integers $\mathbf{d_i}$ hereinafter called elementary challenges; the witness, on the basis of each challenge $\mathbf{d}$, computes a response $\mathbf{D}$,

• either by performing operations of the type:

$$\mathbf{D \equiv r \,.\, Q_1^{d1} \,.\, Q_2^{d2} \,.\, \ldots\, Q_m^{dm} \bmod n}$$

• or

• • by performing operations of the type:

$$\mathbf{D_i \equiv r_i \,.\, Q_{i,1}^{d1} \,.\, Q_{i,2}^{d2} \,.\, \ldots\, Q_{i,m}^{dm} \bmod p_i}$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses $\mathbf{D}$ as there are challenges $\mathbf{d}$ as there are commitments $\mathbf{R}$, each group of numbers $\mathbf{R, d, D}$ forming a triplet referenced $\{\mathbf{R, d, D}\}$ [process specified according to claim 1],

where as the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment $\mathbf{R}$ to the signing device through the interconnection means,

• **Step 2: act of challenge d**

the signing device comprises computation means, hereinafter called the computation means of the signing device, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute a binary train and extract, from this binary train, challenges **d** whose number is equal to the number of commitments **R**,

• **Step 3: act of response D**

the means for the reception of the challenges **d** of the witness device receive each challenge **d** coming from the signing device through the interconnection means,

the means for computing the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, **m** being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $p_1, p_2, \ldots p_f$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \cdot Q_i^v \equiv 1 \text{ . mod } n \text{ or } G_i \equiv Q_i^v \text{ mod } n;$$

v designating a public exponent such that

$$v = 2^k$$

where **k** is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the **f** prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \text{ mod } n \quad \text{and} \quad x^2 \equiv - g_i \text{ mod } n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \text{ mod } n$$

can be resolved in x in the ring of the integers modulo **n**;

said method implements, in the following steps, an entity called a witness having **f** prime factors

$\mathbf{p_i}$ and/or parameters of the Chinese remainders of the prime factors and/or the public modulus $\mathbf{n}$ and/or the $\mathbf{m}$ private values $\mathbf{Q_i}$ and/or the $\mathbf{f.m}$ components $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j} \equiv Q_i \bmod p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent $\mathbf{v}$;

- the witness computes commitments $\mathbf{R}$ in the ring of the integers modulo $\mathbf{n}$; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v \bmod n}$$

where $\mathbf{r}$ is a random value such that $\mathbf{0 < r < n}$,

• or

• • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^v \bmod p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\mathbf{\{r_1, r_2, \ldots r_f\}}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges $\mathbf{d}$, each challenge $\mathbf{d}$ comprising $\mathbf{m}$ integers $\mathbf{d_i}$ hereinafter called elementary challenges; the witness, on the basis of each challenge $\mathbf{d}$, computes a response $\mathbf{D}$,

• either by performing operations of the type:

$$\mathbf{D \equiv r \,.\, Q_1^{d1} \,.\, Q_2^{d2} \,.\, \ldots\, Q_m^{dm} \bmod n}$$

• or

• • by performing operations of the type:

$$\mathbf{D_i \equiv r_i \,.\, Q_{i,1}^{d1} \,.\, Q_{i,2}^{d2} \,.\, \ldots\, Q_{i,m}^{dm} \bmod p_i}$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses $\mathbf{D}$ as there are challenges $\mathbf{d}$ as there are commitments $\mathbf{R}$, each group of numbers $\mathbf{R, d, D}$ forming a triplet referenced $\mathbf{\{R, d, D\}}$ [process specified according to claim 1],

where as the witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses $\mathbf{D}$ to the signing device, through the interconnection means.

09/889918
12 December 2001

S/N unknown

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	GUILLOU et al.	Docket No.:	9320.134USWO
Serial No.:	09/889918	Filed:	July 24, 2001
Int'l Appln No.:	PCT/FR00/00190	Int'l Filing Date:	January 27, 2000
Title:	METHOD FOR PROVING THE AUTHENTICITY OF AN ENTITY.....		

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service, as first class mail, with sufficient postage, in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on October 23, 2001.

By: Todd Michel
Name: Todd Michel

SUPPLEMENTAL PRELIMINARY AMENDMENT

Box PCT
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

In connection with the above-identified application, please enter the following preliminary amendment, which is subsequent to the initial preliminary amendment filed on July 24, 2001, based on the Article 34 amendments, based on claims amended in prosecution of the international application and published in the International Preliminary Examination Report (marked-up copy attached):

IN THE SPECIFICATION

A courtesy copy of the present specification was filed with the application on July 24, 2001. However, the World Intellectual Property Office (WIPO) copy should be relied upon if it is already in the U.S. Patent Office.

IN THE CLAIMS

Please insert the following language to the last page of the TEXT AS AMENDED section that was filed with the above-identified application on July 24, 2001. However, please note that the following language was included in the courtesy copy of the TEXT AS FILED section filed on July 24, 2001:

case where the demonstrator has transmitted the totality of each commitment R

if the transmission means of the demonstrator have received the totality of each commitment **R**, the computation means and the comparison means of the controller device, having **m** public values $\mathbf{G_1, G_2, \ldots, G_m}$, ascertain that each commitment **R** satisfies a relationship of the type

$$\mathbf{R \equiv G_1^{\,d1} \,.\, G_2^{\,d2} \,.\, \ldots\, G_m^{\,dm} \,.\, D^v \bmod n}$$

or a relationship of the type

$$\mathbf{R \equiv D^v / G_1^{\,d1} \,.\, G_2^{\,d2} \,.\, \ldots\, G_m^{\,dm} \,.\, \bmod n}$$

17. Controller device according to claim 15, designed to give proof to an entity, known as a controller, of the integrity of a message **M** associated with an entity known as a demonstrator,

said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to a demonstrator device associated with the demonstrator entity,

said system enabling the execution of the following steps:

• **Steps 1 and 2: act of commitment R, act of challenge d**

said controller device also has means for the reception of tokens **T** coming from the demonstrator device through the connection means,

the controller device has challenge production means for the production, after having received the token **T**, of the challenges **d** in a number equal to the number of commitments **R**, each challenge **d** comprising **m** integers $\mathbf{d_i}$, herein after called elementary challenges,

the controller device also has transmission means, hereinafter called the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means;

• **Steps 3 and 4: act of response D, act of checking**

the controller device also comprises:

- means for the reception of the responses **D** coming from the demonstrator device, through the connection means,

- computation means, hereinafter called the computation means of the controller device, having **m** public values $\mathbf{G_1, G_2, \ldots, G_m}$, to firstly compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$\mathbf{R' \equiv G_1{}^{d1} . G_2{}^{d2} . \ldots G_m{}^{dm} . D^v \bmod n}$$

or a relationship of the type

$$\mathbf{R' \equiv D^v/G_1{}^{d1} . G_2{}^{d2} . \ldots G_m{}^{dm} . \bmod n}$$

then, secondly, compute a token **T'** by applying the hashing function **h** having as arguments the message **M** and all or part of each reconstructed commitment **R'**,

the controller device also comprises:

- comparison means, hereinafter called the comparison means of the controller device, to compare the computed token **T'** with the received token **T**.

18. Controller device according to claim 15, designed to prove the authenticity of the message **M** by checking a signed message by means of an entity called a controller;

the signed message, sent by a signing device associated with a signing entity having a hashing function **h (message, R),** comprising:

- the message **M**,

- the challenges **d** and/or the commitments **R**,

- the responses **D**;

Checking operation

said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to a signing device associated with the signing entity,

said controller device having received the signed message from the signed device, through the connection means,

the controller device comprises:

- computation means, hereinafter called the computation means of the controller device,

- comparison means, hereinafter called the comparison means of the controller device;

• case where the controller device has commitments R, challenges d, responses D

if the controller has commitments **R**, challenges **d**, responses **D**,

• • the computation and comparison means of the controller device ascertain that the commitments **R**, the challenges **d** and the responses **D** satisfy relationships of the type

$$\mathbf{R \equiv G_1^{\ d1} . G_2^{\ d2} . \ldots G_m^{\ dm} . D^v \bmod n}$$

or relationships of the type:

$$\mathbf{R \equiv D^v / G_1^{\ d1} . G_2^{\ d2} . \ldots G_m^{\ dm} . \bmod n}$$

• • the computation and comparison means of the controller device ascertain that the message **M**, the challenges **d** and the commitments **R** satisfy the hashing function

$$\mathbf{d = h\ (message, R)}$$

• case where the controller device has challenges d and responses D

if the controller device has challenges **d** and responses **D**,

• • the computation means of the controller, on the basis of each challenge **d** and each response **D,** compute commitments **R'** satisfying relationships of the type

$$\mathbf{R' \equiv G_1^{\ d1} . G_2^{\ d2} . \ldots G_m^{\ dm} . D^v \bmod n}$$

or relationships of the type:

$$\mathbf{R' \equiv D^v / G_1^{\ d1} . G_2^{\ d2} . \ldots G_m^{\ dm} . \bmod n}$$

• • the computation and comparison means of the controller device ascertain that the message **M** and the challenges **d** satisfy the hashing function:

$$\mathbf{d = h\ (message, R')}$$

• case where the controller device has commitments R and responses D

if the controller device has commitments **R** and responses **D,**

• • the computation means of the controller device apply the hashing function and compute **d'** such that

$$\mathbf{d' = h\ (message, R)}$$

• • the computation and comparison means of the controller device ascertain that the commitments **R,** the challenges **d'** and the responses **D** satisfy relationships of the type

$$\mathbf{R \equiv G_1^{\ d'1} . G_2^{\ d'2} . \ldots G_m^{\ d'm} . D^v \bmod n}$$

or relationships of the type:

$$R \equiv D^{v}/G_1^{\,d'1} \,.\, G_2^{\,d'2} \,.\, \ldots\, G_m^{\,d'm} \,.\, \bmod n$$

Please amend the following claims:

7. (Twice Amended) A system according to claim 6, designed to prove the authenticity of an entity called a demonstrator and an entity called a controller,
said system being such that it comprises:

- a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

- a controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device;

said system enabling the execution of the following steps:

- **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, $\mathbf{m}$ being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus $\mathbf{n}$ constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, $\mathbf{f}$ being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \,.\, Q_i^{\,v} \equiv 1 \,.\, \bmod n \text{ or } G_i \equiv Q_i^{\,v} \bmod n;$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met: neither of the two equations:

$$\mathbf{x^2 \equiv g_i \bmod n} \quad \text{and} \qquad \mathbf{x^2 \equiv - g_i \bmod n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$\mathbf{x^v \equiv g_i^2 \bmod n}$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors $\mathbf{p_i}$ and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values $\mathbf{Q_i}$ and/or the **f.m** components $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j} \equiv Q_i \bmod p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v \bmod n}$$

where **r** is a random value such that $\mathbf{0 < r < n}$,

• or

• • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^v \bmod p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\mathbf{\{r_1, r_2, \ldots r_f\}}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers $\mathbf{d_i}$ hereinafter called elementary challenges; the witness, on the basis of each challenge **d,** computes a response **D,**

• either by performing operations of the type:

$$\mathbf{D \equiv r \,.\, Q_1^{\,d1} \,.\, Q_2^{\,d2} \,.\, \ldots\, Q_m^{\,dm} \bmod n}$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}{}^{d1} \cdot Q_{i,2}{}^{d2} \cdot \ldots Q_{i,m}{}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}**,

where as the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

the demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator, to transmit all or part of each commitment **R** to the controller device through the connection means;

• **Step 2: act of challenge d**

the controller device comprises challenge production means for the production, after receiving all or part of each commitment **R**, of the challenges **d** equal in number to the number of commitments **R**,

the controller device also has transmission means, hereinafter known as the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means.

• **Step 3: act of response D**

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the demonstrator device through the interconnection means,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, **m** being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $p_1, p_2, \ldots p_f$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following

type

$$\mathbf{G_i \,.\, Q_i^{\,v} \equiv 1 \,.\, mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^{\,v}\ mod\ n;}$$

v designating a public exponent such that

$$\mathbf{v} = \mathbf{2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met: neither of the two equations:

$$\mathbf{x^2 \equiv g_i\ mod\ n} \quad \text{and} \qquad \mathbf{x^2 \equiv -\, g_i\ mod\ n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$\mathbf{x^v \equiv g_i^{\,2}\ mod\ n}$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors $\mathbf{p_i}$ and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values $\mathbf{Q_i}$ and/or the **f.m** components $\mathbf{Q_{i,\,j}}$ ($\mathbf{Q_{i,\,j} \equiv Q_i\ mod\ p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v\ mod\ n}$$

where **r** is a random value such that $\mathbf{0 < r < n}$,

• or

• • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^{\,v}\ mod\ p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\{\mathbf{r_1, r_2, \ldots r_f}\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers $\mathbf{d_i}$ hereinafter called elementary challenges; the witness, on the basis of each challenge **d,** computes

a response **D**,

• either by performing operations of the type:

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}**,

• **Step 4: act of checking**

the transmission means of the demonstrator transmit each response **D** to the controller,

the controller device also comprises:

- computation means, hereinafter called the computation means of the controller device,

- comparison means, hereinafter called the comparison means of the controller device,

case where the demonstrator has transmitted a part of each commitment R.

if the transmission means of the demonstrator have transmitted a part of each commitment **R**, the computation means of the controller device, having **m** public values $G_1, G_2, \ldots, G_m$, compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \ldots G_m^{dm} \cdot D^v \bmod n$$

or a relationship of the type

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \ldots G_m^{dm} \cdot \bmod n$$

the comparison means of the controller device compare each reconstructed commitment **R'** with all or part of each commitment **R** received,

case where the demonstrator has transmitted the totality of each commitment R

if the transmission means of the demonstrator have transmitted the totality of each commitment **R**, the computation means and the comparison means of the controller device, having **m** public values $G_1, G_2, \ldots, G_m$, ascertain that each commitment **R** satisfies a relationship of the type

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \ldots G_m^{dm} \cdot D^v \bmod n$$

or a relationship of the type

$$R \equiv D^{v} / G_1^{d1} \,.\, G_2^{d2} \,.\, \ldots \, G_m^{dm} \,.\, \bmod n$$

8. (Twice Amended) System according to claim 6, designed to give proof to an entity, known as a controller, of the integrity of a message **M** associated with an entity known as a demonstrator,

said system being such that it comprises

- a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

- a controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device;

said system enabling the execution of the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, **m** being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $p_1, p_2, \ldots p_f$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \,.\, Q_i^{v} \equiv 1 \,.\, \bmod n \text{ or } G_i \equiv Q_i^{v} \bmod n;$$

v designating a public exponent such that

$$v = 2^{k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i}^2$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$\mathbf{x^2 \equiv g_i \bmod n} \quad \text{and} \quad \mathbf{x^2 \equiv - g_i \bmod n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$\mathbf{x^v \equiv g_i^2 \bmod n}$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors $\mathbf{p_i}$ and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values $\mathbf{Q_i}$ and/or the **f.m** components $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j} \equiv Q_i \bmod p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v \bmod n}$$

where **r** is a random value such that $\mathbf{0 < r < n}$,

• or

• • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^v \bmod p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\{\mathbf{r_1, r_2, \ldots r_f}\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers $\mathbf{d_i}$ hereinafter called elementary challenges; the witness, on the basis of each challenge **d,** computes a response **D,**

• either by performing operations of the type:

$$\mathbf{D \equiv r \,.\, Q_1^{\,d1} \,.\, Q_2^{\,d2} \ldots Q_m^{\,dm} \bmod n}$$

• or

• • by performing operations of the type:

$$\mathbf{D_i \equiv r_i \,.\, Q_{i,1}^{\ d1} \,.\, Q_{i,2}^{\ d2} .\, \ldots\, Q_{i,m}^{\ dm} \bmod p_i}$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}**,

where as the witness device has transmission means, hereinafter called transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

• **Step 2: act of challenge d**

the demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute at least one token **T,**

the demonstrator device also has transmission means, hereinafter known as the transmission means of the demonstrator device, to transmit each token **T** through the connection means to the controller device,

the controller device also has challenge production means for the production, after having received the token **T**, of the challenges **d** in a number equal to the number of commitments **R,**

the controller device also has transmission means, hereinafter called the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means;

• **Step 3: act of response D**

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the demonstrator device through the interconnection means,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following

type

$$G_i \,.\, Q_i^v \equiv 1 \,.\, \mathbf{mod}\ n \text{ or } G_i \equiv Q_i^v\ \mathbf{mod}\ n;$$

v designating a public exponent such that

$$v = 2^k$$

where **k** is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the **f** prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met: neither of the two equations:

$$x^2 \equiv g_i\ \mathbf{mod}\ n \quad \text{and} \quad x^2 \equiv -\, g_i\ \mathbf{mod}\ n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2\ \mathbf{mod}\ n$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or the **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i\ \mathbf{mod}\ p_j$) of the private values Q_i and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v\ \mathbf{mod}\ n$$

where **r** is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v\ \mathbf{mod}\ p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d,** computes

a response **D**,

• either by performing operations of the type:

$$\mathbf{D \equiv r . Q_1^{d1} . Q_2^{d2} . \dots Q_m^{dm} \bmod n}$$

• or

• • by performing operations of the type:

$$\mathbf{D_i \equiv r_i . Q_{i,1}^{d1} . Q_{i,2}^{d2} . \dots Q_{i,m}^{dm} \bmod p_i}$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}**,

• **Step 4: act of checking**

the transmission means of the demonstrator transmit each response **D** to the controller,

the controller device also comprises computation means, hereinafter called the computation means of the controller device, having **m** public values $\mathbf{G_1, G_2, \dots, G_m}$, to firstly compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$\mathbf{R' \equiv G_1^{d1} . G_2^{d2} . \dots G_m^{dm} . D^v \bmod n}$$

or a relationship of the type

$$\mathbf{R' \equiv D^v / G_1^{d1} . G_2^{d2} . \dots G_m^{dm} . \bmod n}$$

then, secondly, compute a token **T'** by applying the hashing function **h** having as arguments the message **M** and all or part of each reconstructed commitment **R'**,

the controller device also has comparison means, hereinafter known as the comparison means of the controller device, to compare the computed token **T'** with the received token **T**.

9. (Twice Amended) System according to claim 6, designed to produce the digital signature of a message **M**, hereinafter known as the signed message, by an entity called a signing entity;

the signed message comprising:

- the message **M**,
- the challenges **d** and/or the commitments **R**,
- the responses **D**;

Signing operation

said system being such that it comprises a signing device associated with the signing entity, said signing device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said system enabling the execution of the following steps:

- **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, $\mathbf{m}$ being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus $\mathbf{n}$ constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, $\mathbf{f}$ being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \cdot Q_i^v \equiv 1 \ . \ mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^v\ mod\ n;}$$

$\mathbf{v}$ designating a public exponent such that

$$\mathbf{v = 2^k}$$

where $\mathbf{k}$ is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the $\mathbf{f}$ prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$\mathbf{x^2 \equiv g_i\ mod\ n} \quad \text{and} \quad \mathbf{x^2 \equiv - g_i\ mod\ n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$\mathbf{x^v \equiv g_i^2\ mod\ n}$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors

$\mathbf{p_i}$ and/or parameters of the Chinese remainders of the prime factors and/or the public modulus $\mathbf{n}$ and/or the $\mathbf{m}$ private values $\mathbf{Q_i}$ and/or the $\mathbf{f.m}$ components $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j} \equiv Q_i \bmod p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent $\mathbf{v}$;

- the witness computes commitments $\mathbf{R}$ in the ring of the integers modulo $\mathbf{n}$; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v \bmod n}$$

where $\mathbf{r}$ is a random value such that $\mathbf{0 < r < n}$,

• or

• • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^{\,v} \bmod p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\{\mathbf{r_1}, \mathbf{r_2}, \ldots \mathbf{r_f}\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges $\mathbf{d}$, each challenge $\mathbf{d}$ comprising $\mathbf{m}$ integers $\mathbf{d_i}$ hereinafter called elementary challenges; the witness, on the basis of each challenge $\mathbf{d}$, computes a response $\mathbf{D}$,

• either by performing operations of the type:

$$\mathbf{D \equiv r \,.\, Q_1^{\,d1} \,.\, Q_2^{\,d2} . \ldots Q_m^{\,dm} \bmod n}$$

• or

• • by performing operations of the type:

$$\mathbf{D_i \equiv r_i \,.\, Q_{i,1}^{\,d1} \,.\, Q_{i,2}^{\,d2} . \ldots Q_{i,m}^{\,dm} \bmod p_i}$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses $\mathbf{D}$ as there are challenges $\mathbf{d}$ as there are commitments $\mathbf{R}$, each group of numbers $\mathbf{R, d, D}$ forming a triplet referenced $\{\mathbf{R, d, D}\}$,

where as the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment $\mathbf{R}$ to the demonstrator device through the interconnection means,

• **Step 2: act of challenge d**

the signing device comprises computation means, hereinafter called the computation means of the signing device, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute a binary train and extract, from this binary train, challenges **d** whose number is equal to the number of commitments **R**,

• **Step 3: act of response D**

the means for the reception of the challenges **d** of the witness device receive each challenge **d** coming from the signing device through the interconnection means,

the means for computing the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \dots Q_m$ and public values $G_1, G_2, \dots G_m$, **m** being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $p_1, p_2, \dots p_f$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \,.\, Q_i^v \equiv 1 \,.\, \text{mod } n \text{ or } G_i \equiv Q_i^v \text{ mod } n;$$

v designating a public exponent such that

$$v = 2^k$$

where **k** is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the **f** prime factors $p_1, p_2, \dots p_f$; the base number g_i being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \text{ mod } n \quad \text{and} \quad x^2 \equiv - g_i \text{ mod } n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \text{ mod } n$$

can be resolved in x in the ring of the integers modulo **n**;

said method implements, in the following steps, an entity called a witness having **f** prime factors

$\mathbf{p_i}$ and/or parameters of the Chinese remainders of the prime factors and/or the public modulus $\mathbf{n}$ and/or the $\mathbf{m}$ private values $\mathbf{Q_i}$ and/or the $\mathbf{f.m}$ components $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j} \equiv Q_i \bmod p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent $\mathbf{v}$;

- the witness computes commitments $\mathbf{R}$ in the ring of the integers modulo $\mathbf{n}$; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v \bmod n}$$

where $\mathbf{r}$ is a random value such that $\mathbf{0 < r < n}$,

• or

• • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^v \bmod p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\mathbf{\{r_1 , r_2 , \ldots r_f\}}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges $\mathbf{d}$, each challenge $\mathbf{d}$ comprising $\mathbf{m}$ integers $\mathbf{d_i}$ hereinafter called elementary challenges; the witness, on the basis of each challenge $\mathbf{d}$, computes a response $\mathbf{D}$,

• either by performing operations of the type:

$$\mathbf{D \equiv r . Q_1^{\,d1} . Q_2^{\,d2} . \ldots Q_m^{\,dm} \bmod n}$$

• or

• • by performing operations of the type:

$$\mathbf{D_i \equiv r_i . Q_{i,1}^{\,d1} . Q_{i,2}^{\,d2} . \ldots Q_{i,m}^{\,dm} \bmod p_i}$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses $\mathbf{D}$ as there are challenges $\mathbf{d}$ as there are commitments $\mathbf{R}$, each group of numbers $\mathbf{R, d, D}$ forming a triplet referenced $\mathbf{\{R, d, D\}}$,

where as the witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses $\mathbf{D}$ to the signing device through the interconnection means.

12. (Twice Amended) A terminal device according to claim 11, designed to prove the authenticity of an entity called a demonstrator to an entity called a controller.
said terminal device being such that it comprises a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and being capable especially of taking the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,
said demonstrator device also comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;
said terminal device enabling the execution of the following steps:

• Step 1: act of commitment R

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \cdot Q_i^v \equiv 1 \,.\, mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^v\ mod\ n;}$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:
neither of the two equations:

$$\mathbf{x^2 \equiv g_i\ mod\ n} \quad \text{and} \quad \mathbf{x^2 \equiv -\ g_i\ mod\ n}$$

can be resolved in x in the ring of integers modulo $\mathbf{n}$

the equation:

$$\mathbf{x^v \equiv g_i^2 \bmod n}$$

can be resolved in x in the ring of the integers modulo $\mathbf{n}$;

said method implements, in the following steps, an entity called a witness having $\mathbf{f}$ prime factors $\mathbf{p_i}$ and/or parameters of the Chinese remainders of the prime factors and/or the public modulus $\mathbf{n}$ and/or the $\mathbf{m}$ private values $\mathbf{Q_i}$ and/or the $\mathbf{f.m}$ components $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j} \equiv Q_i \bmod p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent $\mathbf{v}$;

- the witness computes commitments $\mathbf{R}$ in the ring of the integers modulo $\mathbf{n}$; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v \bmod n}$$

where $\mathbf{r}$ is a random value such that $\mathbf{0 < r < n}$,

• or

• • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^v \bmod p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\mathbf{\{r_1, r_2, \ldots r_f\}}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges $\mathbf{d}$, each challenge $\mathbf{d}$ comprising $\mathbf{m}$ integers $\mathbf{d_i}$ hereinafter called elementary challenges; the witness, on the basis of each challenge $\mathbf{d}$, computes a response $\mathbf{D}$,

• either by performing operations of the type:

$$\mathbf{D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n}$$

• or

• • by performing operations of the type:

$$\mathbf{D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i}$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses $\mathbf{D}$ as there are challenges $\mathbf{d}$ as there are commitments $\mathbf{R}$, each group of numbers $\mathbf{R, d, D}$ forming a triplet referenced $\mathbf{\{R, d, D\}}$,

where as the witness device has transmission means, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

the demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator, to transmit all or part of each commitment **R** to the controller device, through the connection means;

• **Steps 2 and 3: act of challenge d, act of response D**

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the controller device through the connection means between the controller device and the demonstrator device and through the interconnection means between the demonstrator device and the witness device,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \cdot Q_i^v \equiv 1 \ . \ mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^v\ mod\ n;}$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$\mathbf{x^2 \equiv g_i\ mod\ n} \quad \text{and} \quad \mathbf{x^2 \equiv -\ g_i\ mod\ n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or the **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where **r** is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d,** computes a response **D,**

• either by performing operations of the type:

$$D \equiv r \,.\, Q_1^{d1} \,.\, Q_2^{d2} \,.\, \ldots\, Q_m^{dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \,.\, Q_{i,1}^{d1} \,.\, Q_{i,2}^{d2} \,.\, \ldots\, Q_{i,m}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}**,

• **Step 4: act of checking**

the transmission means of the demonstrator transmit each response **D** to the controller that carries out the check.

13. (Twice Amended) Terminal device according to claim 11, designed to give proof to an entity, known as a controller, of the integrity of a message **M** associated with an entity known as a demonstrator,
said terminal device being such that it comprises a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and being capable especially of taking the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,
said demonstrator device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;
said terminal device being used to execute the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, m being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $p_1, p_2, \ldots p_f$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i . Q_i^v \equiv 1 . \bmod n \text{ or } G_i \equiv Q_i^v \bmod n;$$

v designating a public exponent such that

$$v = 2^k$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the $\mathbf{f}$ prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$\mathbf{x^2 \equiv g_i \bmod n} \quad \text{and} \quad \mathbf{x^2 \equiv - g_i \bmod n}$$

can be resolved in x in the ring of integers modulo $\mathbf{n}$

the equation:

$$\mathbf{x^v \equiv g_i^2 \bmod n}$$

can be resolved in x in the ring of the integers modulo $\mathbf{n}$;

said method implements, in the following steps, an entity called a witness having $\mathbf{f}$ prime factors $\mathbf{p_i}$ and/or parameters of the Chinese remainders of the prime factors and/or the public modulus $\mathbf{n}$ and/or the $\mathbf{m}$ private values $\mathbf{Q_i}$ and/or the $\mathbf{f.m}$ components $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j} \equiv Q_i \bmod p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent $\mathbf{v}$;

- the witness computes commitments $\mathbf{R}$ in the ring of the integers modulo $\mathbf{n}$; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v \bmod n}$$

where $\mathbf{r}$ is a random value such that $\mathbf{0 < r < n}$,

• or

• • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^v \bmod p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\{\mathbf{r_1, r_2, \ldots r_f}\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges $\mathbf{d}$, each challenge $\mathbf{d}$ comprising $\mathbf{m}$ integers $\mathbf{d_i}$ hereinafter called elementary challenges; the witness, on the basis of each challenge $\mathbf{d}$, computes a response $\mathbf{D}$,

• either by performing operations of the type:

$$\mathbf{D \equiv r \,.\, Q_1^{\,d1} \,.\, Q_2^{\,d2} \,.\, \ldots\, Q_m^{\,dm} \bmod n}$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{\ d1} \cdot Q_{i,2}^{\ d2} \cdot \ldots Q_{i,m}^{\ dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}**;

where as the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

• **Steps 2 and 3: act of challenge d, act of response D**

the demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute at least one token **T**,

the demonstrator device also has transmission means, hereinafter known as the transmission means of the demonstrator device, to transmit each token **T**, through the connection means, to the controller device,

said controller, after having received the token **T**, produces challenges **d** equal in number to the number of commitments **R**,

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the controller device through the connection means between the controller device and the demonstrator device and through the interconnection means between the demonstrator device and the witness device,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, **m** being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $p_1, p_2, \ldots p_f$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \,.\, Q_i^v \equiv 1 \,.\, \textbf{mod n} \text{ or } G_i \equiv Q_i^v \textbf{ mod n};$$

v designating a public exponent such that

$$v = 2^k$$

where **k** is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the **f** prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met: neither of the two equations:

$$x^2 \equiv g_i \textbf{ mod n} \quad \text{and} \qquad x^2 \equiv - g_i \textbf{ mod n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \textbf{ mod n}$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or the **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \textbf{ mod } p_j$) of the private values Q_i and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \textbf{ mod n}$$

where **r** is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \textbf{ mod } p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d,** computes a response **D,**

• either by performing operations of the type:

$$\mathbf{D} \equiv \mathbf{r} \,.\, \mathbf{Q}_1^{\ d1} \,.\, \mathbf{Q}_2^{\ d2} . \ldots \mathbf{Q}_m^{\ dm} \bmod \mathbf{n}$$

• or

• • by performing operations of the type:

$$\mathbf{D}_i \equiv \mathbf{r}_i \,.\, \mathbf{Q}_{i,1}^{\ d1} \,.\, \mathbf{Q}_{i,2}^{\ d2} . \ldots \mathbf{Q}_{i,m}^{\ dm} \bmod \mathbf{p}_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}**,

• **Step 4: act of checking**

the transmission means of the demonstrator send each response **D** to the controller device which performs the check.

14. (Twice Amended) Terminal device according to claim 11, designed to produce the digital signature of a message **M**, hereinafter known as the signed message, by an entity called a signing entity;

the signed message comprising:

- the message **M**,
- the challenges **d** and/or the commitments **R**,
- the responses **D**;

said terminal device being such that it comprises a signing device associated with the signing entity, said signing device being interconnected with the witness device by interconnection means and possibly taking especially the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said demonstrator device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

Signing operation

said terminal device being used to execute the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \cdot Q_i^v \equiv 1 \cdot mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^v\ mod\ n;}$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$\mathbf{x^2 \equiv g_i\ mod\ n} \quad \text{and} \quad \mathbf{x^2 \equiv -\ g_i\ mod\ n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$\mathbf{x^v \equiv g_i^2\ mod\ n}$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors $\mathbf{p_i}$ and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values $\mathbf{Q_i}$ and/or the **f.m** components $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j} \equiv Q_i\ mod\ p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v\ mod\ n}$$

where $\mathbf{r}$ is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^{\,v} \bmod p_i$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $0 < r_i < p_i$, each $\mathbf{r_i}$ belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers $\mathbf{d_i}$ hereinafter called elementary challenges; the witness, on the basis of each challenge **d,** computes a response **D**,

• either by performing operations of the type:

$$D \equiv r \,.\, Q_1^{\,d1} \,.\, Q_2^{\,d2} . \ldots Q_m^{\,dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \,.\, Q_{i,1}^{\,d1} \,.\, Q_{i,2}^{\,d2} . \ldots Q_{i,m}^{\,dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}**,

where as the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the signing device through the interconnection means,

• **Step 2: act of challenge d**

the signing device comprises computation means, hereinafter called the computation means of the signing device, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute a binary train and extract, from this binary train, challenges **d** whose number is equal to the number of commitments **R,**

• **Step 3: act of response D**

the means for the reception of the challenges **d** of the witness device receive each challenge **d** coming from the signing device through the interconnection means,

the means for computing the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \dots Q_m$ and public values $G_1, G_2, \dots G_m$, **m** being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $p_1, p_2, \dots p_f$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \cdot Q_i^v \equiv 1 \,.\, \bmod n \text{ or } G_i \equiv Q_i^v \bmod n;$$

v designating a public exponent such that

$$v = 2^k$$

where **k** is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the **f** prime factors $p_1, p_2, \dots p_f$; the base number g_i being such that the following two conditions are met: neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv - g_i \bmod n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n**;

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or the **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent **v**;

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where $\mathbf{r}$ is a random value such that $\mathbf{0 < r < n}$,

• or

• • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^{\,v} \bmod p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\mathbf{\{r_1 , r_2 , \ldots r_f\}}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers $\mathbf{d_i}$ hereinafter called elementary challenges; the witness, on the basis of each challenge **d**, computes a response **D**,

• either by performing operations of the type:

$$\mathbf{D \equiv r \,.\, Q_1^{\,d1} \,.\, Q_2^{\,d2} . \ldots Q_m^{\,dm} \bmod n}$$

• or

• • by performing operations of the type:

$$\mathbf{D_i \equiv r_i \,.\, Q_{i,1}^{\,d1} \,.\, Q_{i,2}^{\,d2} . \ldots Q_{i,m}^{\,dm} \bmod p_i}$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}**, where as the witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses **D** to the signing device, through the interconnection means.

REMARKS

The above preliminary amendment is made to insert the pages inadvertantly missing from the TEXT AS AMENDED section filed on July 24, 2001, and to remove multiple dependencies from claims 7, 8, 9, 12, 13 and 14.

Applicants respectfully request that the preliminary amendment described herein be entered into the record prior to calculation of the filing fee and prior to examination and consideration of the above-identified application.

If a telephone conference would be helpful in resolving any issues concerning this communication, please contact Applicants' primary attorney-of record, John J. Gresens (Reg. No. 33,112), at (612) 371.5265.

Respectfully submitted,

MERCHANT & GOULD P.C.
P.O. Box 2903
Minneapolis, Minnesota 55402-0903
(612) 332-5300

Dated: October 23, 2001

By ____________________
John J. Gresens
Reg. No. 33,112

JJG/tvm

MARKED-UP COPY

7. (Twice Amended) A system according to claim 6, designed to prove the authenticity of an entity called a demonstrator and an entity called a controller,

said system being such that it comprises:

- a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

- a controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device;

said system enabling the execution of the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \dots Q_m}$ and public values $\mathbf{G_1, G_2, \dots G_m}$, **m** being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \dots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \,.\, Q_i^{\,v} \equiv 1 \,.\, mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^{\,v}\ mod\ n;}$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \dots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv -\, g_i \bmod n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or the **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where **r** is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d,** computes a response **D**,

• either by performing operations of the type:

$$D \equiv r \,.\, Q_1^{d1} \,.\, Q_2^{d2} . \ldots Q_m^{dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \,.\, Q_{i,1}^{d1} \,.\, Q_{i,2}^{d2} . \ldots Q_{i,m}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** [process specified according to claim 1],

where as the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

the demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator, to transmit all or part of each commitment **R** to the controller device through the connection means;

- **Step 2: act of challenge d**

the controller device comprises challenge production means for the production, after receiving all or part of each commitment **R**, of the challenges **d** equal in number to the number of commitments **R,**

the controller device also has transmission means, hereinafter known as the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means.

- **Step 3: act of response D**

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the demonstrator device through the interconnection means,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \,.\, Q_i^v \equiv 1 \,.\, mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^v\ mod\ n};$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$\mathbf{x^2 \equiv g_i \bmod n} \quad \text{and} \quad \mathbf{x^2 \equiv - g_i \bmod n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$\mathbf{x^v \equiv g_i^2 \bmod n}$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors $\mathbf{p_i}$ and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values $\mathbf{Q_i}$ and/or the **f.m** components $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j} \equiv Q_i \bmod p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v \bmod n}$$

where **r** is a random value such that $\mathbf{0 < r < n}$,

• or

• • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^v \bmod p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\mathbf{\{r_1 , r_2 , \ldots r_f\}}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers $\mathbf{d_i}$ hereinafter called elementary challenges; the witness, on the basis of each challenge **d,** computes a response **D,**

• either by performing operations of the type:

$$\mathbf{D \equiv r \,.\, Q_1^{\,d1} \,.\, Q_2^{\,d2} . \ldots Q_m^{\,dm} \bmod n}$$

• or

• • by performing operations of the type:

$$\mathbf{D_i \equiv r_i \,.\, Q_{i,1}^{\,d1} \,.\, Q_{i,2}^{\,d2} .\, \ldots\, Q_{i,m}^{\,dm} \bmod p_i}$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** [process specified according to claim 1],

• **Step 4: act of checking**

the transmission means of the demonstrator transmit each response **D** to the controller,

the controller device also comprises:

- computation means, hereinafter called the computation means of the controller device,

- comparison means, hereinafter called the comparison means of the controller device,

case where the demonstrator has transmitted a part of each commitment R.

if the transmission means of the demonstrator have transmitted a part of each commitment **R**, the computation means of the controller device, having **m** public values $\mathbf{G_1, G_2, \ldots, G_m}$, compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$\mathbf{R' \equiv G_1^{\,d1} \,.\, G_2^{\,d2} \,. \ldots\, G_m^{\,dm} \,.\, D^v \bmod n}$$

or a relationship of the type

$$\mathbf{R' \equiv D^v / G_1^{\,d1} \,.\, G_2^{\,d2} \,. \ldots\, G_m^{\,dm} \,.\, \bmod n}$$

the comparison means of the controller device compare each reconstructed commitment **R'** with all or part of each commitment **R** received,

case where the demonstrator has transmitted the totality of each commitment R

if the transmission means of the demonstrator have transmitted the totality of each commitment **R**, the computation means and the comparison means of the controller device, having **m** public values $\mathbf{G_1, G_2, \ldots, G_m}$, ascertain that each commitment **R** satisfies a relationship of the type

$$\mathbf{R \equiv G_1^{\,d1} \,.\, G_2^{\,d2} \,. \ldots\, G_m^{\,dm} \,.\, D^v \bmod n}$$

or a relationship of the type

$$\mathbf{R \equiv D^v / G_1^{\,d1} \,.\, G_2^{\,d2} \,. \ldots\, G_m^{\,dm} \,.\, \bmod n}$$

8. (Twice Amended) System according to claim 6, designed to give proof to an entity, known as a controller, of the integrity of a message **M** associated with an entity known as a demonstrator,

said system being such that it comprises

- a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

- a controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device;

said system enabling the execution of the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \,.\, Q_i^v \equiv 1 \,.\, mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^v\ mod\ n;}$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \qquad x^2 \equiv - g_i \bmod n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or the **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where **r** is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d,** computes a response **D,**

• either by performing operations of the type:

$$D \equiv r \,.\, Q_1^{d1} \,.\, Q_2^{d2} . \ldots Q_m^{dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \,.\, Q_{i,1}^{d1} \,.\, Q_{i,2}^{d2} . \ldots Q_{i,m}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** [process specified in claim 1],

where as the witness device has transmission means, hereinafter called transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

• **Step 2: act of challenge d**

the demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute at least one token **T,**

the demonstrator device also has transmission means, hereinafter known as the transmission means of the demonstrator device, to transmit each token **T** through the connection means to the controller device,

the controller device also has challenge production means for the production, after having received the token **T**, of the challenges **d** in a number equal to the number of commitments **R,**

the controller device also has transmission means, hereinafter called the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means;

• **Step 3: act of response D**

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the demonstrator device through the interconnection means,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i . Q_i^v \equiv 1 . mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^v\ mod\ n;}$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \dots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$\mathbf{x^2 \equiv g_i\ mod\ n} \quad \text{and} \quad \mathbf{x^2 \equiv - g_i\ mod\ n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$\mathbf{x^v \equiv g_i^2\ mod\ n}$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors $\mathbf{p_i}$ and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values $\mathbf{Q_i}$ and/or the **f.m** components $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j} \equiv Q_i\ mod\ p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v\ mod\ n}$$

where **r** is a random value such that $\mathbf{0 < r < n}$,

• or

• • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^v\ mod\ p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\mathbf{\{r_1, r_2, \dots r_f\}}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers $\mathbf{d_i}$ hereinafter called elementary challenges; the witness, on the basis of each challenge **d,** computes a response **D**,

• either by performing operations of the type:

$$\mathbf{D \equiv r \,.\, Q_1^{\ d1} \,.\, Q_2^{\ d2} \,.\, \ldots\, Q_m^{\ dm} \bmod n}$$

• or

• • by performing operations of the type:

$$\mathbf{D_i \equiv r_i \,.\, Q_{i,1}^{\ d1} \,.\, Q_{i,2}^{\ d2} \,.\, \ldots\, Q_{i,m}^{\ dm} \bmod p_i}$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** [process specified according to claim 1],

• **Step 4: act of checking**

the transmission means of the demonstrator transmit each response **D** to the controller,

the controller device also comprises computation means, hereinafter called the computation means of the controller device, having **m** public values $\mathbf{G_1, G_2, \ldots, G_m}$, to firstly compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$\mathbf{R' \equiv G_1^{\ d1} \,.\, G_2^{\ d2} \,.\, \ldots\, G_m^{\ dm} \,.\, D^v \bmod n}$$

or a relationship of the type

$$\mathbf{R' \equiv D^v / G_1^{\ d1} \,.\, G_2^{\ d2} \,.\, \ldots\, G_m^{\ dm} \,.\, \bmod n}$$

then, secondly, compute a token **T'** by applying the hashing function **h** having as arguments the message **M** and all or part of each reconstructed commitment **R'**,

the controller device also has comparison means, hereinafter known as the comparison means of the controller device, to compare the computed token **T'** with the received token **T**.

9. (Twice Amended) System according to claim 6, designed to produce the digital signature of a message **M**, hereinafter known as the signed message, by an entity called a signing entity;

the signed message comprising:

- the message **M**,
- the challenges **d** and/or the commitments **R**,
- the responses **D**;

Signing operation

said system being such that it comprises a signing device associated with the signing entity, said signing device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said system enabling the execution of the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \,.\, Q_i^{\,v} \equiv 1 \,.\, mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^{\,v}\ mod\ n;}$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i}^2$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$\mathbf{x^2 \equiv g_i\ mod\ n} \quad \text{and} \quad \mathbf{x^2 \equiv -\, g_i\ mod\ n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$\mathbf{x^v \equiv g_i^{\,2}\ mod\ n}$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors

p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or the $f.m$ components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent v;

- the witness computes commitments R in the ring of the integers modulo n; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where r is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges d, each challenge d comprising m integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge d, computes a response D,

• either by performing operations of the type:

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses D as there are challenges d as there are commitments R, each group of numbers R, d, D forming a triplet referenced $\{R, d, D\}$ [process specified according to claim 1],

where as the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment R to the demonstrator device through the interconnection means,

• **Step 2: act of challenge d**

the signing device comprises computation means, hereinafter called the computation means of the signing device, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute a binary train and extract, from this binary train, challenges **d** whose number is equal to the number of commitments **R**,

• **Step 3: act of response D**

the means for the reception of the challenges **d** of the witness device receive each challenge **d** coming from the signing device through the interconnection means,

the means for computing the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \dots Q_m}$ and public values $\mathbf{G_1, G_2, \dots G_m}$, **m** being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \dots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \,.\, Q_i^v \equiv 1 \,.\, mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^v\ mod\ n};$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \dots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$\mathbf{x^2 \equiv g_i\ mod\ n} \quad \text{and} \quad \mathbf{x^2 \equiv -\ g_i\ mod\ n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$\mathbf{x^v \equiv g_i^2\ mod\ n}$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors

$\mathbf{p_i}$ and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values $\mathbf{Q_i}$ and/or the **f.m** components $\mathbf{Q_{i,\,j}}$ ($\mathbf{Q_{i,\,j} \equiv Q_i \bmod p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent **v**;

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v \bmod n}$$

where **r** is a random value such that $\mathbf{0 < r < n}$,

• or

• • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^{\,v} \bmod p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\{\mathbf{r_1, r_2, \ldots r_f}\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers $\mathbf{d_i}$ hereinafter called elementary challenges; the witness, on the basis of each challenge **d**, computes a response **D**,

• either by performing operations of the type:

$$\mathbf{D \equiv r \,.\, Q_1^{\ d1} \,.\, Q_2^{\ d2} \,. \ldots\, Q_m^{\ dm} \bmod n}$$

• or

• • by performing operations of the type:

$$\mathbf{D_i \equiv r_i \,.\, Q_{i,1}^{\ d1} \,.\, Q_{i,2}^{\ d2} \,. \ldots\, Q_{i,m}^{\ dm} \bmod p_i}$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** [process specified according to claim 1],

where as the witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses **D** to the signing device through the interconnection means.

12. (Twice Amended) A terminal device according to claim 11, designed to prove the authenticity of an entity called a demonstrator to an entity called a controller.

said terminal device being such that it comprises a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and being capable especially of taking the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said demonstrator device also comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

said terminal device enabling the execution of the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, $\mathbf{m}$ being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus $\mathbf{n}$ constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, $\mathbf{f}$ being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \cdot Q_i^v \equiv 1 \;.\; mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^v\ mod\ n;}$$

$\mathbf{v}$ designating a public exponent such that

$$\mathbf{v = 2^k}$$

where $\mathbf{k}$ is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the $\mathbf{f}$ prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$\mathbf{x^2 \equiv g_i\ mod\ n} \quad \text{and} \quad \mathbf{x^2 \equiv -\ g_i\ mod\ n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or the **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where **r** is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d,** computes a response **D**,

• either by performing operations of the type:

$$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** [process specified according to claim 1],

where as the witness device has transmission means, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

the demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator, to transmit all or part of each commitment **R** to the controller device, through the connection means;

- **Steps 2 and 3: act of challenge d, act of response D**

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the controller device through the connection means between the controller device and the demonstrator device and through the interconnection means between the demonstrator device and the witness device,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$, **m** being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $p_1, p_2, \ldots p_f$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \,.\, Q_i^v \equiv 1 \,.\, \bmod n \text{ or } G_i \equiv Q_i^v \bmod n;$$

v designating a public exponent such that

$$v = 2^k$$

where **k** is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the **f** prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met:

neither of the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv -g_i \bmod n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or the **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where **r** is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d,** computes a response **D,**

• either by performing operations of the type:

$$D \equiv r \,.\, Q_1^{d1} \,.\, Q_2^{d2} \,.\, \ldots\, Q_m^{dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \,.\, Q_{i,1}^{d1} \,.\, Q_{i,2}^{d2} \,.\, \ldots\, Q_{i,m}^{dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** [process specified according to claim 1],

• **Step 4: act of checking**

the transmission means of the demonstrator transmit each response **D** to the controller that carries out the check.

13. (Twice Amended) Terminal device according to claim 11, designed to give proof to an entity, known as a controller, of the integrity of a message **M** associated with an entity known as a demonstrator,

said terminal device being such that it comprises a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and being capable especially of taking the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said demonstrator device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

said terminal device being used to execute the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \cdot Q_i^v \equiv 1 \text{ . mod } n \text{ or } G_i \equiv Q_i^v \text{ mod } n;$$

v designating a public exponent such that

$$v = 2^k$$

where **k** is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the **f** prime factors $p_1, p_2, \ldots p_f$; the base number g_i being such that the following two conditions are met: neither of the two equations:

$$x^2 \equiv g_i \text{ mod } n \quad \text{and} \quad x^2 \equiv - g_i \text{ mod } n$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$x^v \equiv g_i^2 \text{ mod } n$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or the **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \text{ mod } p_j$) of the private values Q_i and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$R \equiv r^v \text{ mod } n$$

where **r** is a random value such that $0 < r < n$,

• or

• • by performing operations of the type:

$$R_i \equiv r_i^v \text{ mod } p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d**, computes a response **D**,

• either by performing operations of the type:

$$\mathbf{D \equiv r \cdot Q_1^{\ d1} \cdot Q_2^{\ d2} \cdot \ldots Q_m^{\ dm} \bmod n}$$

• or

• • by performing operations of the type:

$$\mathbf{D_i \equiv r_i \cdot Q_{i,1}^{\ d1} \cdot Q_{i,2}^{\ d2} \cdot \ldots Q_{i,m}^{\ dm} \bmod p_i}$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** [process specified according to claim 1];

where as the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

• **Steps 2 and 3: act of challenge d, act of response D**

the demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute at least one token **T**,

the demonstrator device also has transmission means, hereinafter known as the transmission means of the demonstrator device, to transmit each token **T,** through the connection means, to the controller device,

said controller, after having received the token **T**, produces challenges **d** equal in number to the number of commitments **R**,

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the controller device through the connection means between the controller device and the demonstrator device and through the interconnection means between the demonstrator device and the witness device,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m**

being greater than or equal to 1 |, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \cdot Q_i^v \equiv 1 \ . \ mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^v\ mod\ n;}$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met: neither of the two equations:

$$\mathbf{x^2 \equiv g_i\ mod\ n} \quad \text{and} \quad \mathbf{x^2 \equiv -\ g_i\ mod\ n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$\mathbf{x^v \equiv g_i^2\ mod\ n}$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors $\mathbf{p_i}$ and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values $\mathbf{Q_i}$ and/or the **f.m** components $\mathbf{Q_{i,\,j}}$ ($\mathbf{Q_{i,\,j} \equiv Q_i\ mod\ p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent **v;**

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v\ mod\ n}$$

where **r** is a random value such that $\mathbf{0 < r < n}$,

• or

• • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^v\ mod\ p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$

belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge **d,** computes a response **D**,

• either by performing operations of the type:

$$D \equiv r \,.\, Q_1^{\ d1} \,.\, Q_2^{\ d2} \,.\, \ldots\, Q_m^{\ dm} \bmod n$$

• or

• • by performing operations of the type:

$$D_i \equiv r_i \,.\, Q_{i,1}^{\ d1} \,.\, Q_{i,2}^{\ d2} \,.\, \ldots\, Q_{i,m}^{\ dm} \bmod p_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** [process specified according to claim 1],

• **Step 4: act of checking**

the transmission means of the demonstrator send each response **D** to the controller device which performs the check.

14. (Twice Amended) Terminal device according to claim 11, designed to produce the digital signature of a message **M**, hereinafter known as the signed message, by an entity called a signing entity;

the signed message comprising:

- the message **M**,
- the challenges **d** and/or the commitments **R**,
- the responses **D**;

said terminal device being such that it comprises a signing device associated with the signing entity, said signing device being interconnected with the witness device by interconnection means and possibly taking especially the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said demonstrator device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

Signing operation

said terminal device being used to execute the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or

- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \cdot Q_i^v \equiv 1 \;.\; mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^v\ mod\ n;}$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$\mathbf{x^2 \equiv g_i\ mod\ n} \text{ and } \mathbf{x^2 \equiv -\,g_i\ mod\ n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$\mathbf{x^v \equiv g_i^2\ mod\ n}$$

can be resolved in x in the ring of the integers modulo **n;**

said method implements, in the following steps, an entity called a witness having **f** prime factors

$\mathbf{p_i}$ and/or parameters of the Chinese remainders of the prime factors and/or the public modulus $\mathbf{n}$ and/or the $\mathbf{m}$ private values $\mathbf{Q_i}$ and/or the $\mathbf{f.m}$ components $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j} \equiv Q_i \bmod p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent $\mathbf{v}$;

- the witness computes commitments $\mathbf{R}$ in the ring of the integers modulo $\mathbf{n}$; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v \bmod n}$$

where $\mathbf{r}$ is a random value such that $\mathbf{0 < r < n}$,

• or

• • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^v \bmod p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\{\mathbf{r_1}, \mathbf{r_2}, \dots \mathbf{r_f}\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges $\mathbf{d}$, each challenge $\mathbf{d}$ comprising $\mathbf{m}$ integers $\mathbf{d_i}$ hereinafter called elementary challenges; the witness, on the basis of each challenge $\mathbf{d}$, computes a response $\mathbf{D}$,

• either by performing operations of the type:

$$\mathbf{D \equiv r \,.\, Q_1^{d1} \,.\, Q_2^{d2} \,.\, \dots\, Q_m^{dm} \bmod n}$$

• or

• • by performing operations of the type:

$$\mathbf{D_i \equiv r_i \,.\, Q_{i,1}^{d1} \,.\, Q_{i,2}^{d2} \,.\, \dots\, Q_{i,m}^{dm} \bmod p_i}$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses $\mathbf{D}$ as there are challenges $\mathbf{d}$ as there are commitments $\mathbf{R}$, each group of numbers $\mathbf{R, d, D}$ forming a triplet referenced $\{\mathbf{R, d, D}\}$ [process specified according to claim 1],

where as the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment $\mathbf{R}$ to the signing device through the interconnection means,

• **Step 2: act of challenge d**

the signing device comprises computation means, hereinafter called the computation means of the signing device, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute a binary train and extract, from this binary train, challenges **d** whose number is equal to the number of commitments **R**,

• **Step 3: act of response D**

the means for the reception of the challenges **d** of the witness device receive each challenge **d** coming from the signing device through the interconnection means,

the means for computing the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$, **m** being greater than or equal to 1, or of the parameters derived from these values,

- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$, **f** being greater than or equal to 2;

said modulus, said exponent and said values being related by relations of the following type

$$\mathbf{G_i \,.\, Q_i^v \equiv 1 \,.\, mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^v\ mod\ n};$$

v designating a public exponent such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1;

said public value $\mathbf{G_i}$ being the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$; the base number $\mathbf{g_i}$ being such that the following two conditions are met:

neither of the two equations:

$$\mathbf{x^2 \equiv g_i\ mod\ n} \quad \text{and} \quad \mathbf{x^2 \equiv -\ g_i\ mod\ n}$$

can be resolved in x in the ring of integers modulo **n**

the equation:

$$\mathbf{x^v \equiv g_i^2\ mod\ n}$$

can be resolved in x in the ring of the integers modulo **n**;

said method implements, in the following steps, an entity called a witness having **f** prime factors

$\mathbf{p_i}$ and/or parameters of the Chinese remainders of the prime factors and/or the public modulus $\mathbf{n}$ and/or the $\mathbf{m}$ private values $\mathbf{Q_i}$ and/or the $\mathbf{f.m}$ components $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j} \equiv Q_i \bmod p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent $\mathbf{v}$;

- the witness computes commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v \bmod n}$$

where **r** is a random value such that $\mathbf{0 < r < n}$,

• or

• • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^{\,v} \bmod p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\mathbf{\{r_1 , r_2 , \ldots r_f\}}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers $\mathbf{d_i}$ hereinafter called elementary challenges; the witness, on the basis of each challenge **d**, computes a response **D**,

• either by performing operations of the type:

$$\mathbf{D \equiv r \,.\, Q_1^{\,d1} \,.\, Q_2^{\,d2} . \ldots Q_m^{\,dm} \bmod n}$$

• or

• • by performing operations of the type:

$$\mathbf{D_i \equiv r_i \,.\, Q_{i,1}^{\,d1} \,.\, Q_{i,2}^{\,d2} . \ldots Q_{i,m}^{\,dm} \bmod p_i}$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}** [process specified according to claim 1],

where as the witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses **D** to the signing device, through the interconnection means.

09/889918
JC17 Rec'd PCT/PTO 24 JUL 2001

Method for proving the authenticity of an entity and/or the integrity of a message by means of a public exponent equal to the power of two

The present invention relates to the methods, systems and devices designed to prove the authenticity of an entity and/or the integrity and/or authenticity of a message.

The patent EP 0 311 470 B1, whose inventors are Louis Guillou and Jean-Jacques Quisquater, describes such a method. Hereinafter, reference shall be made to their work by the terms "GQ patent" or "GQ method". Hereinafter, the expression "GQ2", or "GQ2 invention" or "GQ2 technology" shall be used to describe the present invention.

According to the GQ method, an entity known as a "trusted authority" assigns an identity to each entity called a "witness" and computes its RSA signature. In a customizing process, the trusted authority gives the witness an identity and signature. Thereafter, the witness declares the following: "Here is my identity; I know its RSA signature ". The witness proves that he knows the RSA signature of his identity without revealing this signature. Through the RSA public identification key distributed by the trusted authority, an entity known as a "controller" ascertains, without obtaining knowledge thereof, that the RSA signature corresponds to the declared identity. The mechanisms using the GQ method run "without transfer of knowledge". According to the GQ method, the witness does not know the RSA private key with which the trusted authority signs a large number of identities.

The GQ technology described here above makes use of RSA technology. However, while the RSA technology truly depends on the factorization of the modulus n, this dependence is not an equivalence, indeed far from it, as can be seen in what are called multiplicative attacks against various standards of digital signatures implementing the RSA technology.

The goal of the GQ2 technology is twofold: firstly to improve the performance characteristics of RSA technology and secondly to avert the problems inherent in RSA technology. Knowledge of the GQ2 private key is equivalent to knowledge of the factorization of the modulus n. Any attack on the triplets GQ2 leads to the

factorization of the modulus n: this time there is equivalence. With the GQ2 technology, the work load is reduced for the signing or self-authenticating entity and for the controller entity. Through a better use of the problem of factorizing in terms of both security and performance, the GQ2 technology averts the drawbacks of RSA technology.

The GQ method implements modulo computations of numbers comprising 512 bits or more. These computations relate to numbers having substantially the same size raised to powers of the order of $2^{16} + 1$. Now, existing microelectronic infrastructures, especially in the field of bank cards, make use of monolithic self-programmable microprocessors without arithmetical coprocessors. The work load related to multiple arithmetical applications involved in methods such as the GQ method leads to computation times which, in certain cases, prove to be disadvantageous for consumers using bank cards to pay for their purchases. It may be recalled here that, in seeking to increase the security of payment cards, the banking authorities have raised a problem that is particularly difficult to resolve. Indeed, two apparently contradictory questions have to be resolved: on the one hand, increasing security by using increasingly lengthy and distinct keys for each card while, on the other hand, preventing the work load from leading to excessive computation times for the user. This problem becomes especially acute inasmuch as it is also necessary to take account of the existing infrastructure and the existing microprocessor components.

The GQ2 technology provides a solution to this problem while boosting security.

Method

More particularly, the invention relates to a method designed to prove the following to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

This proof is established by means of all or part of the following parameters or derivatives of these parameters:

- $\mathbf{m}$ pairs of private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$ ($\mathbf{m}$ being greater than or equal to 1),

- a public modulus $\mathbf{n}$ constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$ ($\mathbf{f}$ being greater than or equal to 2),

- a public exponent $\mathbf{v}$.

Said modulus, said exponent and said values are related by relations of the type

$$\mathbf{G_i \cdot Q_i^v \equiv 1 \cdot mod\ n} \text{ or } \mathbf{G_i \equiv Q_i^v\ mod\ n}.$$

Said exponent $\mathbf{v}$ is such that

$$\mathbf{v = 2^k}$$

where $\mathbf{k}$ is a security parameter greater than 1.

Said public value $\mathbf{G_i}$ is the square $\mathbf{g_i^2}$ of a base number $\mathbf{g_i}$ smaller than the $\mathbf{f}$ prime factors $\mathbf{p_1, p_2, \ldots p_f}$. The base number $\mathbf{g_i}$ is such that

the two equations:

$$\mathbf{x^2 \equiv g_i\ mod\ n} \quad \text{and} \quad \mathbf{x^2 \equiv -\ g_i\ mod\ n}$$

cannot be resolved in x in the ring of integers modulo $\mathbf{n}$ and such that:

the equation:

$$\mathbf{x^v \equiv g_i^2\ mod\ n}$$

can be resolved in x in the ring of the integers modulo $\mathbf{n}$.

Said method implements an entity called a witness in the following steps. Said witness entity has $\mathbf{f}$ prime factors $\mathbf{p_i}$ and/or parameters of the Chinese remainders of the prime factors and/or the public modulus $\mathbf{n}$ and/or the $\mathbf{m}$ private values $\mathbf{Q_i}$ and/or the $\mathbf{f.m}$ components $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j} \equiv Q_i\ mod\ p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent $\mathbf{v}$.

The witness computes commitments $\mathbf{R}$ in the ring of integers modulo $\mathbf{n}$. Each commitment is computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v\ mod\ n}$$

where $\mathbf{r}$ is a random value such that $\mathbf{0 < r < n}$,

• or

• • by performing operations of the type:

$$\mathbf{R_i \equiv r_i^{v} \bmod p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\{\mathbf{r_1, r_2, \ldots r_f}\}$,

• • then by applying the Chinese remainder method.

The witness receives one or more challenges **d**. Each challenge **d** comprises **m** integers $\mathbf{d_i}$ hereinafter called elementary challenges. The witness, on the basis of each challenge **d**, computes a response **D**,

• either by performing operations of the type:

$$\mathbf{D \equiv r \,.\, Q_1^{\,d1} \,.\, Q_2^{\,d2} \ldots Q_m^{\,dm} \bmod n}$$

• or

• • by performing operations of the type:

$$\mathbf{D_i \equiv r_i \,.\, Q_{i,1}^{\,d1} \,.\, Q_{i,2}^{\,d2} \ldots Q_{i,m}^{\,dm} \bmod p_i}$$

and then by applying the Chinese remainder method.

The method is such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}.**

Case of the proof of the authenticity of an entity

In a first alternative embodiment, the method according to the invention is designed to prove the authenticity of an entity known as a demonstrator to an entity known as the controller. Said demonstrator entity comprises the witness. Said demonstrator and controller entities execute the following steps:

• **Step 1: act of commitment R**

At each call, the witness computes each commitment **R** by applying the process specified here above. The demonstrator sends the controller all or part of each commitment **R**.

• **Step 2: act of challenge d**

The controller, after having received all or part of each commitment **R**, produces challenges **d** whose number is equal to the number of commitments **R** and sends the challenges **d** to the demonstrator.

• **Step 3: act of response D**

The witness computes the responses **D** from the challenges **d** by applying the above-specified process.

• **Step 4: act of checking**

The demonstrator sends each response **D** to the controller.

First case: the demonstrator has transmitted a part of each commitment R

If the demonstrator has transmitted a part of each commitment **R**, the controller, having the **m** public values $G_1, G_2, \ldots, G_m$, computes a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

or a relationship of the type

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

The controller ascertains that each reconstructed commitment **R'** reproduces all or part of each commitment **R** that has been transmitted to it.

Second case: the demonstrator has transmitted the totality of each commitment R

If the demonstrator has transmitted the totality of each commitment **R**, the controller, having the **m** public values $G_1, G_2, \ldots, G_m$, ascertains that each commitment **R** satisfies a relationship of the type

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

or a relationship of the type

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

Case of the proof of the integrity of the message

In a second alternative embodiment capable of being combined with a first one, the method of the invention is designed to provide proof to an entity, known as the controller entity, of the integrity of a message **M** associated with an entity called a demonstrator entity. Said demonstrator entity comprises the witness. Said demonstrator and controller entities perform the following steps:

• **Step 1: act of commitment R**

At each call, the witness computes each commitment **R** by applying the process specified here above.

• **Step 2: act of challenge d**

The demonstrator applies a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute at least one token **T**. The demonstrator sends the token **T** to the controller. The controller, after having received a token **T**, produces challenges **d** equal in number to the number of commitments **R** and sends the challenges **d** to the demonstrator.

• **Step 3: act of response D**

The witness computes the responses **D** from the challenges **d** by applying the above-specified process.

• **Step 4: act of checking**

The demonstrator sends each response **D** to the controller. The controller, having the **m** public values $G_1, G_2, \ldots, G_m$, computes a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$R' \equiv G_1^{\ d1} \,.\, G_2^{\ d2} \,.\, \ldots\, G_m^{\ dm} \,.\, D^v \bmod n$$

or a relationship of the type

$$R' \equiv D^v / G_1^{\ d1} \,.\, G_2^{\ d2} \,.\, \ldots\, G_m^{\ dm} \,.\, \bmod n$$

Then the controller applies the hashing function **h** whose arguments are the message **M** and all or part of each reconstructed commitment **R'** to reconstruct the token **T'**. Then the controller ascertains that the token **T'** is identical to the token **T** transmitted.

Digital signature of a message and proof of its authenticity

In a third alternative embodiment capable of being combined with the above two, the method according to the invention 1 is designed to produce the digital signature of a message **M** by an entity known as the signing entity. Said signing entity includes the witness.

Signing operation

Said signing entity executes a signing operation in order to obtain a signed message comprising:

- the message **M**,
- the challenges **d** and/or the commitments **R**,
- the responses **D**.

Said signing entity executes the signing operation by implementing the following steps:

• **Step 1: act of commitment R**

At each call, the witness computes each commitment **R** by applying the process specified here above.

• **Step 2: act of challenge d**

The signing party applies a hashing function **h** whose arguments are the message **M** and each commitment **R** to obtain a binary train. From this binary train, the signing party extracts challenges **d** whose number is equal to the number of commitments **R**.

• **Step 3: act of response D**

The witness computes the responses **D** from the challenges **d** by applying the above-specified process.

Checking operation

To prove the authenticity of the message **M**, an entity called a controller checks the signed message. Said controller entity having the signed message carries out a checking operation by proceeding as follows.

• **Case where the controller has commitments R, challenges d, responses D**

If the controller has commitments **R**, challenges **d**, responses **D**, the controller ascertains that the commitments **R**, the challenges **d** and the responses **D** satisfy relationships of the type

$$\mathbf{R \equiv G_1{}^{d1} . G_2{}^{d2} . \ldots G_m{}^{dm} . D^v \bmod n}$$

or relationships of the type:

$$\mathbf{R \equiv D^v / G_1{}^{d1} . G_2{}^{d2} . \ldots G_m{}^{dm} . \bmod n}$$

Then the controller ascertains that the message **M**, the challenges **d** and the commitments **R** satisfy the hashing function:

$$d = h\ (\text{message}, R)$$

• **Case where the controller has challenges d and responses D**

If the controller has challenges **d** and responses **D**, the controller reconstructs, on the basis of each challenge **d** and each response **D**, commitments **R'** satisfying relationships of the type

$$R' \equiv G_1^{\ d1} . G_2^{\ d2} . \ldots G_m^{\ dm} . D^v \bmod n$$

or relationships of the type:

$$R' \equiv D^v / G_1^{\ d1} . G_2^{\ d2} . \ldots G_m^{\ dm} . \bmod n$$

Then the controller ascertains that the message **M** and the challenges **d** satisfy the hashing function:

$$d = h\ (\text{message}, R')$$

• **Case where the controller has commitments R and responses D**

If the controller has commitments **R** and responses **D**, the controller applies the hashing function and reconstructs **d'**

$$d' = h\ (\text{message}, R)$$

Then the controller device ascertains that the commitments **R**, the challenges **d'** and the responses **D** satisfy relationships of the type

$$R \equiv G_1^{\ d'1} . G_2^{\ d'2} . \ldots G_m^{\ d'm} . D^v \bmod n$$

or relationships of the type:

$$R \equiv D^v / G_1^{\ d'1} . G_2^{\ d'2} . \ldots G_m^{\ d'm} . \bmod n$$

System

The present invention also relates to a system designed to prove the following to a controller server:

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

This proof is established by means of all or part of the following parameters or derivatives of these parameters:

- **m** pairs of private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$

(**m** being greater than or equal to 1),

- a public modulus **n** constituted by the product of said **f** prime factors $\mathbf{p_1}, \mathbf{p_2}, \ldots \mathbf{p_f}$ (**f** being greater than or equal to 2),
- a public exponent **v**.

Said modulus, said exponent and said values are linked by relations of the type

$$\mathbf{G_i \cdot Q_i^v \equiv 1 \ . \bmod n} \text{ or } \mathbf{G_i \equiv Q_i^v \bmod n} \ .$$

Said exponent **v** is such that

$$\mathbf{v = 2^k}$$

where **k** is a security parameter greater than 1.

Said public value $\mathbf{G_i}$ is the square $\mathbf{g_i^2}$ of the base number $\mathbf{g_i}$ smaller than the **f** prime factors $\mathbf{p_1}, \mathbf{p_2}, \ldots \mathbf{p_f}$. The base number $\mathbf{g_i}$ is such that the two equations:

$$\mathbf{x^2 \equiv g_i \bmod n} \quad \text{and} \quad \mathbf{x^2 \equiv - g_i \bmod n}$$

cannot be resolved in x in the ring of integers modulo **n** and such that the equation:

$$\mathbf{x^v \equiv g_i^2 \bmod n}$$

can be resolved in x in the ring of the integers modulo **n.**

Said system comprises a witness device, contained especially in a nomad object which, for example, takes the form of a microprocessor-based bank card. The witness device comprises a memory zone containing the **f** prime factors $\mathbf{p_i}$ and/or the parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values $\mathbf{Q_i}$ and/or **f.m** components $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j} \equiv Q_i \bmod p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent **v**. The witness device also comprises:

- random value production means, hereinafter called random value production means of the witness device,
- computation means, hereinafter called means for the computation of commitments **R** of the witness device.

The computation means compute commitments **R** in the ring of integers modulo **n**. Each commitment is computed:

- either by performing operations of the type:

$$\mathbf{R \equiv r^v \bmod n}$$

where **r** is a random value produced by the random value production means, r being such that $\mathbf{0 < r < n}$,

• or by performing operations of the type:

$$\mathbf{R_i \equiv r_i^v \bmod p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\mathbf{\{r_1 , r_2 , \ldots r_f\}}$, then by applying the Chinese remainder method.

The witness device also comprises:

- reception means hereinafter called the means for the reception of the challenges **d** of the witness device, to receive one or more challenges **d**; each challenge **d** comprising **m** integers $\mathbf{d_i}$ hereinafter called elementary challenges.

- computation means, hereinafter called means for the computation of the responses **D** of the witness device for the computation, on the basis of each challenge **d, of** a response **D**,

• either by performing operations of the type:

$$\mathbf{D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \ldots Q_m^{dm} \bmod n}$$

• or by performing operations of the type:

$$\mathbf{D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot \ldots Q_{i,m}^{dm} \bmod p_i}$$

and then by applying the Chinese remainder method.

The witness device also comprises transmission means to transmit one or more commitments **R** and one or more responses **D**. There are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}.**

Case of the proof of the authenticity of an entity

In a first alternative embodiment, the system according to the invention is designed to prove the authenticity of an entity called a demonstrator to an entity called a controller.

Said system is such that it comprises a demonstrator device associated with a demonstrator entity. Said demonstrator device is interconnected with the witness device by interconnection means. It may especially take the form of logic

microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card.

Said system also comprises a controller device associated with the controller entity. Said controller device especially takes the form of a terminal or remote server. Said controller device comprises connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device.

Said system is used to execute the following steps:

• **Step 1: act of commitment R**

At each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified here above. The witness device has means of transmission, hereinafter called transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means. The demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator, to transmit all or part of each commitment **R** to the controller device through the connection means.

• **Step 2: act of challenge d**

The controller device comprises challenge production means for the production, after receiving all or part of each commitment **R**, of the challenges **d** equal in number to the number of commitments **R**. The controller device also has transmission means, hereinafter known as the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means.

• **Step 3: act of response D**

The means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the demonstrator device through the interconnection means. The means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified here above.

• **Step 4: act of checking**

The transmission means of the demonstrator transmit each response **D** to the controller. The controller device also comprises:

- computation means, hereinafter called the computation means of the controller device,
- comparison means, hereinafter called the comparison means of the controller device.

First case: the demonstrator has transmitted a part of each commitment R.

If the transmission means of the demonstrator have transmitted a part of each commitment **R**, the computation means of the controller device, having **m** public values $G_1, G_2, \ldots, G_m$, compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

or a relationship of the type

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

The comparison means of the controller device compare each reconstructed commitment **R'** with all or part of each commitment **R** received.

Second case: the demonstrator has transmitted the totality of each commitment R

If the transmission means of the demonstrator have transmitted the totality of each commitment **R**, the computation means and the comparison means of the controller device, having **m** public values $G_1, G_2, \ldots, G_m$, ascertain that each commitment **R** satisfies a relationship of the type

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

or a relationship of the type

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

Case of the proof of the integrity of a message

In a second alternative embodiment capable of being combined with the first one, the system according to the invention is designed to give proof to an entity, known as a controller, of the integrity of a message **M** associated with an entity

known as a demonstrator. Said system is such that it comprises a demonstrator device associated with the demonstrator entity. Said demonstrator device is interconnected with the witness device by interconnection means. Said demonstrator device may especially take the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card. Said system also comprises a controller device associated with the controller entity. Said controller device especially takes the form of a terminal or remote server. Said controller device comprises connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device.

Said system is used to execute the following steps:

• **Step 1: act of commitment R**

At each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified here above. The witness device has means of transmission, hereinafter called transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means.

• **Step 2: act of challenge d**

The demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute at least one token **T**. The demonstrator device also has transmission means, hereinafter known as the transmission means of the demonstrator device, to transmit each token **T** through the connection means to the controller device. The controller device also has challenge production means for the production, after having received the token **T**, of the challenges **d** in a number equal to the number of commitments **R**. The controller device also has transmission means, hereinafter called the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means.

• **Step 3: act of response D**

The means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the demonstrator device through the interconnection means. The means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified here above.

• Step 4: act of checking

The transmission means of the demonstrator transmit each response **D** to the controller. The controller device also comprises computation means, hereinafter called the computation means of the controller device, having **m** public values G_1, G_2, ..., G_m, to firstly compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$R' \equiv G_1^{\,d1} \,.\, G_2^{\,d2} \,. \ldots G_m^{\,dm} \,.\, D^v \bmod n$$

or a relationship of the type

$$R' \equiv D^v / G_1^{\,d1} \,.\, G_2^{\,d2} \,. \ldots G_m^{\,dm} \,. \bmod n$$

then, secondly, compute a token **T'** by applying the hashing function **h** having as arguments the message **M** and all or part of each reconstructed commitment **R'**.

The controller device also has comparison means, hereinafter known as the comparison means of the controller device, to compare the computed token **T'** with the received token **T**.

Digital signature of a message and proof of its authenticity

In a third alternative embodiment capable of being combined with either or both of the first two embodiments, the system according to the invention is designed to prove the digital signature of a message **M**, hereinafter known as a signed message, by an entity called a signing entity. The signed message comprises:

- the message **M**,
- the challenges **d** and/or the commitments **R**,
- the responses **D**.

Signing operation

Said system is such that it comprises a signing device associated with the signing entity. Said signing device is interconnected with the witness device by

interconnection means. It may especially take the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card.

Said system is used to execute the following steps:

• **Step 1: act of commitment R**

At each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified here above. The witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means.

• **Step 2: act of challenge d**

The signing device comprises computation means, hereinafter called the computation means of the signing device, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute a binary train and extract, from this binary train, challenges **d** whose number is equal to the number of commitments **R**.

• **Step 3: act of response D**

The means for the reception of the challenges **d** of the witness device receive each challenge **d** coming from the signing device through the interconnection means. The means for computing the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified here above.

The witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses **D** to the signing device through the interconnection means.

Checking operation

To prove the authenticity of the message **M**, an entity known as the controller checks the signed message.

The system comprises a controller device associated with the controller entity. Said controller device especially takes the form of a terminal or remote server. Said controller device comprises connection means for its electrical,

electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the signing device.

The signing device associated with the signing entity comprises transmission means, hereinafter known as the transmission means of the signing device, for the transmission, to the controller device, of the signed message through the connection means. Thus the controller device has a signed message comprising:

- the message **M**,
- the challenges **d** and/or the commitments **R**,
- the responses **D**.

The controller device comprises:

- computation means hereinafter called the computation means of the controller device,
- comparison means, hereinafter called the comparison means of the controller device.

• Case where the controller device has commitments R, challenges d, responses D

Should the controller device have commitments **R**, challenges **d**, responses **D**, the computation and comparison means of the controller device ascertain that the commitments **R**, the challenges **d** and the responses **D** satisfy relationships of the type

$$\mathbf{R \equiv G_1^{\,d1} . G_2^{\,d2} . \dots G_m^{\,dm} . D^v \bmod n}$$

or relationships of the type

$$\mathbf{R \equiv D^v/G_1^{\,d1} . G_2^{\,d2} . \dots G_m^{\,dm} . \bmod n}$$

Then, the computation and comparison means of the controller device ascertain that the message **M**, the challenges **d** and the commitments **R** satisfy the hashing function:

$$\mathbf{d = h\ (message, R)}$$

• Case where the controller device has challenges d and responses D

If the controller has challenges **d** and responses **D**, the controller reconstructs, on the basis of each challenge **d** and each response **D**, commitments **R'** satisfying relationships of the type

$$\mathbf{R' \equiv G_1^{\,d1} . G_2^{\,d2} . \dots G_m^{\,dm} . D^v \bmod n}$$

or relationships of the type:

$$\mathbf{R' \equiv D^v / G_1^{\,d1} . G_2^{\,d2} . \dots G_m^{\,dm} . \bmod n}$$

Then the controller ascertains that the message **M** and the challenges **d** satisfy the hashing function:

$$\mathbf{d = h\ (message, R')}$$

• Case where the controller has commitments R and responses D

If the controller has commitments **R** and responses **D**, the computation means of the controller device apply the hashing function and compute **d'** such that

$$\mathbf{d' = h\ (message, R)}$$

Then the computation and comparison means of the controller device ascertain that the commitments **R**, the challenges **d'** and the responses **D** satisfy relationships of the type

$$\mathbf{R \equiv G_1^{\,d1} . G_2^{\,d2} . \dots G_m^{\,dm} . D^v \bmod n}$$

or relationships of the type:

$$\mathbf{R \equiv D^v / G_1^{\,d1} . G_2^{\,d2} . \dots G_m^{\,dm} . \bmod n}$$

Terminal Device

The invention also relates to a terminal device associated with an entity. The terminal device especially take the form of a nomad object, for example the form of a microprocessor in a microprocessor-based bank card. The terminal device is designed to prove the following to a controller server:

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity.

This proof is established by means of all or part of the following parameters or derivatives of these parameters:

- **m** pairs of private values $\mathbf{Q_1, Q_2, \dots Q_m}$ and public values $\mathbf{G_1, G_2, \dots G_m}$

(**m** being greater than or equal to 1),

- a public modulus **n** constituted by the product of said **f** prime factors $p_1, p_2, \ldots p_f$ (**f** being greater than or equal to 2),

- a public exponent **v**.

Said modulus, said exponent and said values are related by relations of the type

$$G_i \cdot Q_i^v \equiv 1 \ . \ \mathrm{mod}\ n \text{ or } G_i \equiv Q_i^v \ \mathrm{mod}\ n\ .$$

Said exponent **v** is such that

$$v = 2^k$$

where **k** is a security parameter greater than 1.

Said public value G_i is the square g_i^2 of the base number g_i smaller than the **f** prime factors $p_1, p_2, \ldots p_f$. The base number g_i is such that:

the two equations:

$$x^2 \equiv g_i \ \mathrm{mod}\ n \quad \text{and} \qquad x^2 \equiv - g_i \ \mathrm{mod}\ n$$

cannot be resolved in x in the ring of integers modulo **n** and such that

the equation:

$$x^v \equiv g_i^2 \ \mathrm{mod}\ n$$

can be resolved in x in the ring of the integers modulo **n**.

Said terminal device comprises a witness device comprising a memory zone containing the **f** prime factors p_i and/or the parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \ \mathrm{mod}\ p_j$) of the private values Q_i and of the public exponent **v**.

The witness device also comprises:

- random value production means, hereinafter called random value production means of the witness device,

- computation means, hereinafter called means for the computation of commitments **R** of the witness device, to compute commitments **R** in the ring of the integers modulo **n**.

Each commitment is computed:

• either by performing operations of the type:

$$\mathbf{R} \equiv \mathbf{r}^{\mathbf{v}} \bmod \mathbf{n}$$

where $\mathbf{r}$ is a random value produced by the random value production means, r being such that $\mathbf{0} < \mathbf{r} < \mathbf{n}$,

• or by performing operations of the type:

$$\mathbf{R_i} \equiv \mathbf{r_i}^{\mathbf{v}} \bmod \mathbf{p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0} < \mathbf{r_i} < \mathbf{p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\{\mathbf{r_1}, \mathbf{r_2}, \ldots \mathbf{r_f}\}$ produced by the random value production means, then by applying the Chinese remainder method.

The witness device also comprises:

- reception means hereinafter called the means for the reception of the challenges **d** of the witness device, to receive one or more challenges **d**; each challenge **d** comprising **m** integers $\mathbf{d_i}$ hereinafter called elementary challenges.

- computation means, hereinafter called means for the computation of the responses **D** of the witness device, for the computation, on the basis of each challenge **d, of** a response **D**,

• either by performing operations of the type:

$$\mathbf{D} \equiv \mathbf{r} \cdot \mathbf{Q_1}^{\mathbf{d1}} \cdot \mathbf{Q_2}^{\mathbf{d2}} \cdot \ldots \mathbf{Q_m}^{\mathbf{dm}} \bmod \mathbf{n}$$

• or by performing operations of the type:

$$\mathbf{D_i} \equiv \mathbf{r_i} \cdot \mathbf{Q_{i,1}}^{\mathbf{d1}} \cdot \mathbf{Q_{i,2}}^{\mathbf{d2}} \cdot \ldots \mathbf{Q_{i,m}}^{\mathbf{dm}} \bmod \mathbf{p_i}$$

and then by applying the Chinese remainder method.

Said witness device also comprises transmission means to transmit one or more commitments **R** and one or more responses **D**. There are as many responses **D** as there are challenges **d** as there are commitments **R**. Each group of numbers **R, d, D** forms a triplet referenced **{R, d, D}.**

Case of the proof of the authenticity of an entity

In a first alternative embodiment, the terminal device according to the invention is designed to prove the authenticity of an entity called a demonstrator to an entity called a controller.

Said terminal device is such that it comprises a demonstrator device associated with a demonstrator entity. Said demonstrator device is interconnected

with the witness device by interconnection means. It may especially take the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card.

Said demonstrator device also comprises connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity. Said controller device especially takes the form of a terminal or remote server.

Said terminal device is used to execute the following steps:

• Step 1: act of commitment R

At each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified here above.

The witness device has means of transmission, hereinafter called transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means. The demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator, to transmit all or part of each commitment **R** to the controller device, through the connection means.

• Steps 2 and 3: act of challenge d, act of response D

The means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the controller device through the connection means between the controller device and the demonstrator device and through the interconnection means between the demonstrator device and the witness device. The means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified here above.

• Step 4: act of checking

The transmission means of the demonstrator transmit each response **D** to the controller that carries out the check.

Case of the proof of the integrity of a message

In a second alternative embodiment capable of being combined with the first one, the terminal device according to the invention is designed to give proof to an entity, known as a controller, of the integrity of a message **M** associated with an entity known as a demonstrator. Said terminal device is such that it comprises a demonstrator device associated with the demonstrator entity. Said demonstrator device is interconnected with the witness device by interconnection means. It may especially take the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card. Said demonstrator device comprises connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity. Said controller device especially takes the form of a terminal or remote server.

Said terminal device is used to execute the following steps:

• Step 1: act of commitment R

At each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified here above. The witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means.

• Steps 2 and 3: act of challenge d, act of response D

The demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute at least one token **T**. The demonstrator device also has transmission means, hereinafter known as the transmission means of the demonstrator device, to transmit each token **T**, through the connection means, to the controller device.

Said controller, after having received the token **T**, produces challenges **d** in a number equal to the number of commitments **R**

The means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the controller device through the connection means

between the controller device and the demonstrator device and through the interconnection means between the demonstrator device and the witness device. The means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified here above.

• Step 4: act of checking

The transmission means of the demonstrator send each response **D** to the controller device which performs the check.

Digital signature of a message and proof of its authenticity

In a third alternative embodiment capable of being combined with either or both of the first two embodiments, the terminal device according to the invention is designed to produce the digital signature of a message **M**, hereinafter known as a signed message, by an entity called a signing entity. The signed message comprises:

- the message **M**,
- the challenges **d** and/or the commitments **R**,
- the responses **D**.

Said terminal device is such that it comprises a signing device associated with the signing entity. Said signing device is interconnected with the witness device by interconnection means. It may especially take the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card. Said demonstrator device comprises connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity. Said controller device especially takes the form of a terminal or remote server.

Signing operation

Said terminal device is used to execute the following steps:

• Step 1: act of commitment R

At each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified here above. The witness device has means of transmission, hereinafter called the transmission

means of the witness device, to transmit all or part of each commitment **R** to the signing device through the interconnection means.

• **Step 2: act of challenge d**

The signing device comprises computation means, hereinafter called the computation means of the signing device, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute a binary train and extract, from this binary train, challenges **d** whose number is equal to the number of commitments **R**.

• **Step 3: act of response D**

The means for the reception of the challenges **d** of the witness device receive each challenge **d** coming from the signing device through the interconnection means. The means for computing the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified here above. The witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses **D** to the signing device, through the interconnection means.

Controller Device

The invention also relates to a controller device. The controller device may especially take the form of a terminal or remote server associated with a controller entity. The controller device is designed to check:

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity.

This proof is established by means of all or part of the following parameters or derivatives of these parameters:

- **m** pairs of public values $G_1, G_2, \ldots G_m$ (**m** being greater than or equal to 1),
- a public modulus **n** constituted by the product of said **f** prime factors $p_1, p_2, \ldots p_f$ (**f** being greater than or equal to 2), unknown to the controller device and to the associated controller entity,
- a public exponent **v**.

Said modulus, said exponent and said values are related by relations of the type

$$G_i \cdot Q_i^v \equiv 1 \ . \ \text{mod } n \text{ or } G_i \equiv Q_i^v \text{ mod } n \ .$$

where Q_i designates a private value, unknown to the controller device, associated with the public value G_i.

The exponent **v** is such that

$$v = 2^k$$

where **k** is a security parameter greater than 1.

Said public value G_i is the square g_i^2 of a base number g_i smaller than the **f** prime factors $p_1, p_2, \ldots p_f$. The base number g_i is such that

the two equations:

$$x^2 \equiv g_i \text{ mod } n \quad \text{and} \quad x^2 \equiv - g_i \text{ mod } n$$

cannot be resolved in x in the ring of integers modulo **n** and such that:

the equation:

$$x^v \equiv g_i^2 \text{ mod } n$$

can be resolved in x in the ring of the integers modulo **n.**

Case of the proof of the authenticity of an entity

In a first alternative embodiment, the controller device according to the invention is designed to prove the authenticity of an entity called a demonstrator and an entity called a controller.

Said controller device comprises connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to a demonstrator device associated with the demonstrator entity.

Said controller device is used to execute the following steps:

• **Steps 1 and 2: act of commitment R, act of challenge d**

Said controller device also has means for the reception of all or part of the commitments **R** coming from the demonstrator device through the connection means.

The controller device has challenge production means for the production, after receiving all or part of each commitment **R**, of the challenges **d** in a number equal to the number of commitments **R**, each challenge **d** comprising **m** integers d_i hereinafter called elementary challenges.

The controller device also has transmission means, hereinafter called transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means.

• **Steps 3 and 4: act of response D, act of checking**

The controller device also comprises:

- means for the reception of the responses D coming from the demonstrator device, through the connection means,

- computation means, hereinafter called the computation means of the controller device,

- comparison means, hereinafter called the comparison means of the controller device.

First case: the demonstrator has transmitted a part of each commitment R.

If the reception means of the demonstrator have received a part of each commitment **R**, the computation means of the controller device, having **m** public values $G_1, G_2, \ldots, G_m$, compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

or a relationship of the type

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

The comparison means of the controller device compare each reconstructed commitment **R'** with all or part of each commitment **R** received.

Second case: the demonstrator has transmitted the totality of each commitment R

If the transmission means of the demonstrator have transmitted the totality of each commitment **R**, the computation means and the comparison means of the controller device, having **m** public values $G_1, G_2, \ldots, G_m$, ascertain that each commitment **R** satisfies a relationship of the type

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

or a relationship of the type

$$R \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \ldots G_m^{dm} \cdot \bmod n$$

Case of the proof of the integrity of a message

In a second alternative embodiment capable of being combined with the first one, the controller device according to the invention is designed to give proof to an entity, known as a controller, of the integrity of a message **M** associated with an entity known as a demonstrator.

Said controller device comprises connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to a demonstrator device associated with the demonstrator entity.

Said system is used to execute the following steps:

• **Steps 1 and 2: act of commitment R, act of challenge d**

Said controller device also has means for the reception of tokens **T** coming from the demonstrator device through the connection means. The controller device has challenge production means for the production, after having received the token **T**, of the challenges **d** in a number equal to the number of commitments **R**, each challenge **d** comprising **m** integers d_i, herein after called elementary challenges. The controller device also has transmission means, hereinafter called the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means.

• **Steps 3 and 4: act of response D, act of checking**

The controller device also comprises means for the reception of the responses **D** coming from the demonstrator device, through the connection means. Said controller device also comprises computation means, hereinafter called the computation means of the controller device, having **m** public values $G_1, G_2, \ldots, G_m$, to firstly compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot \ldots G_m^{dm} \cdot D^v \bmod n$$

or a relationship of the type

$$R' \equiv D^v / G_1^{d1} \cdot G_2^{d2} \cdot \ldots G_m^{dm} \cdot \bmod n$$

then, secondly, compute a token **T'** by applying the hashing function **h** having as arguments the message **M** and all or part of each reconstructed commitment **R'**.

The controller device also has comparison means, hereinafter called the comparison means of the controller device, to compare the computed token **T'** with the received token **T**.

Digital signature of a message and proof of its authenticity

In a third alternative embodiment capable of being combined with either or both of the first two embodiments, the controller device according to the invention is designed to prove the authenticity of the message **M** by checking a signed message by means of an entity called a controller.

The signed message, sent by a signing device associated with a signing entity having a hashing function **h (message, R)** comprises:

- the message **M**,
- the challenges **d** and/or the commitments **R**,
- the responses **D**.

Checking operation

Said controller device comprises connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to a signing device associated with the signing entity. Said controller device receives the signed message from the signed device, through the connection means.

The controller device comprises:

- computation means, hereinafter called the computation means of the controller device,

- comparison means, hereinafter called the comparison means of the controller device.

• Case where the controller device has commitments R, challenges d, responses D

If the controller has commitments **R**, challenges **d**, responses **D**, the computation and comparison means of the controller device ascertain that the

commitments **R**, the challenges **d** and the responses **D** satisfy relationships of the type

$$R \equiv G_1{}^{d1} . G_2{}^{d2} . \ldots G_m{}^{dm} . D^v \bmod n$$

or relationships of the type:

$$R \equiv D^v / G_1{}^{d1} . G_2{}^{d2} . \ldots G_m{}^{dm} . \bmod n$$

Then the computation and comparison means of the controller device ascertain that the message **M**, the challenges **d** and the commitments **R** satisfy the hashing function:

$$d' = h\ (\text{message}, R)$$

• **Case where the controller device has challenges d and responses D**

If the controller device has challenges **d** and responses **D**, the computation means of the controller, on the basis of each challenge **d** and each response **D**, compute commitments **R'** satisfying relationships of the type

$$R' \equiv G_1{}^{d1} . G_2{}^{d2} . \ldots G_m{}^{dm} . D^v \bmod n$$

or relationships of the type:

$$R' \equiv D^v / G_1{}^{d1} . G_2{}^{d2} . \ldots G_m{}^{dm} . \bmod n$$

Then the computation and comparison means of the controller device ascertain that the message **M** and the challenges **d** satisfy the hashing function:

$$d = h\ (\text{message}, R')$$

• **Case where the controller device has commitments R and responses D**

If the controller device has commitments **R** and responses **D**, the computation means of the controller device apply the hashing function and compute **d'** such that

$$d = h\ (\text{message}, R)$$

Then the computation and comparison means of the controller device ascertain that the commitments **R**, the challenges **d'** and the responses **D** satisfy relationships of the type

$$R \equiv G_1{}^{d'1} . G_2{}^{d'2} . \ldots G_m{}^{d'm} . D^v \bmod n$$

or relationships of the type:

$$R \equiv D^v / G_1{}^{d'1} . G_2{}^{d'2} . \ldots G_m{}^{d'm} . \bmod n$$

Description

The goal of GQ technology may be recalled: it is the dynamic authentication of entities and associated messages as well as the digital signature of messages.

The standard version of GQ technology makes use of RSA technology. However, although the RSA technology truly depends on factorizing, this dependence is not an equivalence, far from it, as can be shown from attacks, known as multiplicative attacks, against various digital signature standards implementing RSA technology.

In the context of GQ2 technology, the present part of the invention relates more specifically to the use of sets of GQ2 keys in the context of dynamic authentication and digital signature. The GQ2 technology does not use RSA technology. The goal is a twofold one: first to improve performance with respect to RSA technology and secondly to prevent problems inherent in RSA technology. The GQ2 private key is the factorization of the modulus n. Any attack on the GQ2 triplets amounts to the factorizing of the modulus n: this time there is equivalence. With the GQ2 technology, the work load is reduced both for the entity that signs or is authenticated and for the one that checks. Through an improved use of the problem of factorization, in terms of both security and performance, the GQ2 technology rivals the RSA technology.

The GQ2 technology uses one or more small integers greater than 1, for example m small integers ($m \geq 1$) called base numbers and referenced g_i. Since the base numbers are fixed from g_i to g_m with $m > 1$, a public verification key $\langle v, n \rangle$ is chosen as follows. The public verification exponent v is 2^k where k is a small integer greater than 1 ($k \geq 2$). The public modulus n is the product of at least two prime factors greater than the base numbers, for example f prime factors ($f \geq 2$) referenced by p_j, from $p_1 \ldots p_f$. The f prime factors are chosen so that the public modulus n has the following properties with respect to each of the m base numbers from g_1 to g_m.

- Firstly, the equations (1) and (2) cannot be resolved in x in the ring of the integers modulo n, that is to say that g_i and $-g_i$ are two non-quadratic residues (mod n).

$$x^2 \equiv g_i \pmod{n} \qquad (1)$$
$$x^2 \equiv -g_i \pmod{n} \qquad (2)$$

- Secondly, the equation (3) can be resolved in x in the ring of the integers modulo n.

$$x^{2^k} \equiv g_i^2 \pmod{n} \qquad (3)$$

Since the public verification key $\langle v, n \rangle$ is fixed according to the base numbers from g_1 to g_m with $m \geq 1$, each base number g_i determines a pair of values GQ2 comprising a public value G_i and a private value Q_i: giving m pairs referenced G_1 Q_1 to G_m Q_m. The public value G_i is the square of the base number g_i: giving $G_i = g_i^2$. The private value Q_i is one of the solutions to the equation (3) or else the inverse (mod n) of such a solution.

Just as the modulus n is broken down into f prime factors, the ring of the integers modulo n are broken down into f Galois fields, from CG(p_1) to CG(p_f). Here are the projections of the equations (1), (2) and (3) in CG(p_j).

$$x^2 \equiv g_i \pmod{p_j} \qquad (1.a)$$
$$x^2 \equiv -g_i \pmod{p_j} \qquad (2.a)$$
$$x^{2^k} \equiv g_i^2 \pmod{p_j} \qquad (3.a)$$

Each private value Q_i can be represented uniquely by f private components, one per prime factor: $Q_{i,j} \equiv Q_i \pmod{p_j}$. Each private component $Q_{i,j}$ is a solution to the equation (3.a) or else the inverse (mod p_j) of such a solution. After all the possible solutions to each equation (3.a) have been computed, the Chinese remainder technique sets up all the possible values for each private value Q_i on the basis of f components of $Q_{i,1}$ to $Q_{i,f}$: Q_i = Chinese remainders ($Q_{i,1}$, $Q_{i,2}$, ... $Q_{i,f}$) so as to obtain all the possible solutions to the equation (3).

The following is the Chinese remainder technique: let there be two positive integers that are mutually prime numbers a and b such that $0 < a < b$, and two components X_a from 0 to $a-1$ and X_b from 0 to $b-1$. It is required to determine X = Chinese remainders (X_a, X_b), namely the unique number X from 0 to $a.b-1$ such that $X_a \equiv X \pmod{a}$ and $X_b \equiv X \pmod{b}$. The following is the Chinese remainder parameter: $\alpha \equiv \{b \pmod{a}\}^{-1} \pmod{a}$. The following is the Chinese remainder

operation: $\varepsilon \equiv X_b \pmod a$; $\delta = X_a - \varepsilon$; if δ is negative, replace δ by $\delta + a$; $\gamma \equiv \alpha \,.\, \delta \pmod a$; $X = \gamma \,.\, b + X_b$.

When the prime factors are arranged in rising order, from the smallest p_1 to the greater p_f, the Chinese remainder parameters can be the following (there are $f-1$ of them, namely one less than prime factors). The first Chinese remainder parameter is $\alpha \equiv \{p_2 \pmod{p_1}\}^{-1} \pmod{p_1}$. The second Chinese remainder parameter is $\beta \equiv \{p_1.p_2 \pmod{p_3}\}^{-1} \pmod{p_3}$. The i–th Chinese remainder parameter is $\lambda \equiv \{p_1.p_2. \ldots p_{i-1} \pmod{p_i}\}^{-1} \pmod{p_i}$. And so on and so forth. Finally, in $f-1$ Chinese remainder operations, a first result (mod p_2 times p_1) is obtained with the first parameter and then a second result (mod $p_1.p_2$ times p_3) with the second parameter and so on and so forth until a result (mod $p_1. \ldots p_{f-1}$ times p_f), namely (mod n).

There are several possible depictions of the private key GQ2, which expresses **the polymorphic nature of the private key GQ2**. The various depictions prove to be equivalent: they all amount to knowledge of the factorization of the module n which is the true private GQ2 key. <u>If the depiction truly affects the behavior of the signing entity or self-authenticating entity, it does not affect the behavior of the controller entity</u>.

Here are the main three possible depictions of the GQ2 private key.

1) <u>The standard representation in GQ technology</u> consists of the storage of m private values Q_i and the public verification key <v, n>; in GQ2, this depiction is rivalled by the following two. 2) <u>The optimal representation in terms of work load</u> consists in storing the public exponent v, the f prime factors p_j, $m.f$ private components Q_{ij} and f-1 parameters of the Chinese remainders. 3) <u>The optimal representation in terms of private key size</u> consists in storing the public exponent v, the m basic numbers g_i and the f prime factors p_j, then in starting each use by setting up either m private values Q_i and the module n to return to the first depiction or else $m.f$ private components $Q_{i,j}$ and f-1 parameters of the Chinese remainders to return to the second one.

The signing or self-authenticating entities can all use the same base numbers. Unless otherwise indicated, the m base numbers from g_1 to g_m can then advantageously be the m first prime numbers;

Because the security of the dynamic authentication mechanism or digital signature mechanism is equivalent to knowledge of a breakdown of the modulus, the GQ2 technology cannot be used to simply distinguish two entities using the same modulus. Generally, each entity that authenticates itself or signs has its own GQ2 modulus. However, it is possible to specify GQ2 moduli with four prime factors, two of which are known by an entity and the other two by another entity.

Here is a first set of GQ2 keys with $\boldsymbol{k} = \mathbf{6}$, giving $v = 64$, $\boldsymbol{m} = \mathbf{3}$, giving three base: $g_1 = 3$, $g_2 = 5$ et $g_3 = 7$, and $\boldsymbol{f} = \mathbf{3}$, namely a modulus with three prime factors: two congruent to 3 (mod 4) and one to 5 (mod 8). It must be noted that $g = 2$ is incompatible with a prime factor congruent to 5 (mod 8).

p_1 = 03CD2F4F21E0EAD60266D5CFCEBB6954683493E2E833

p_2 = 0583B097E8D8D777BAB3874F2E76659BB614F985EC1B

p_3 = 0C363CD93D6B3FEC78EE13D7BE9D84354B8FDD6DA1FD

$n = p_1 \cdot p_2 \cdot p_3$ = FFFF81CEA149DCF2F72EB449C5724742FE2A3630D9
02CC00EAFEE1B957F3BDC49BE9CBD4D94467B72AF28CFBB26144
CDF4BBDBA3C97578E29CC9BBEE8FB6DDDD

$Q_{1,1}$ = 0279C60D216696CD6F7526E23512DAE090CFF879FDDE

$Q_{2,1}$ = 7C977FC38F8413A284E9CE4EDEF4AEF35BF7793B89

$Q_{3,1}$ = 6FB3B9CO5A03D7CADA9A3425571EF5ECC54D7A7B6F

$Q_{1,2}$ = 0388EC6AA1E87613D832E2B80E5AE8C1DF2E74BFF502

$Q_{2,2}$ = 04792CE70284D16E9A158C688A7B3FEAF9C40056469E

$Q_{3,2}$ = FDC4A8E53E185A4DA793E93BEE5C636DA731BDCA4E

$Q_{1,3}$ = 07BC1AB048A2EAFDAB59BD40CCF2F657AD8A6B573BDE

$Q_{2,3}$ = 0AE8551E116A3AC089566DFDB3AE003CF174FC4E4877

$Q_{3,3}$ = 01682D490041913A4EA5B80D16B685E4A6DD88070501

Q_1 = D7E1CAF28192CED6549FF457708D50A7481572DD5F2C335D8
C69E22521B510B64454FB7A19AEC8D06985558E764C6991B05FC2A

C74D9743435AB4D7CF0FF6557

Q_2 = CB1ED6B1DD649B89B9638DC33876C98AC7AF689E9D1359E4 DB17563B9B3DC582D5271949F3DBA5A70C108F561A274405A5CB8 82288273ADE67353A5BC316C093

Q_3 = 09AA6F4930E51A70CCDFA77442B10770DD1CD77490E3398A AD9DC50249C34312915E55917A1ED4D83AA3D607E3EB5C8B197 697238537FE7A0195C5E8373EB74D

The following is a second set of GQ2 keys, with $\boldsymbol{k} = \mathbf{9}$, that is $v = 512$, $\boldsymbol{m} = \mathbf{2}$, that is two base numbers: $g_1 = 2$ and $g_2 = 3$, and $\boldsymbol{f} = \mathbf{3}$, giving a modulus with three prime factors congruent to 3 (mod 4).

p_1 = 03852103E40CD4F06FA7BAA9CC8D5BCE96E3984570CB

p_2 = 062AC9EC42AA3E688DC2BC871C8315CB939089B61DD7

p_3 = 0BCADEC219F1DFBB8AB5FE808A0FFCB53458284ED8E3

$n = p_1 \cdot p_2 \cdot p_3$ = FFFF5401ECD9E537F167A80C0A9111986F7A8EBA4D

6698AD68FF670DE5D9D77DFF00716DC7539F7CBBCF969E73A0C49

761B276A8E6B6977A21D51669D039F1D7

$Q_{1,1}$ = 0260BC7243C22450D566B5C6EF74AA29F2B927AF68E1

$Q_{2,1}$ = 0326C12FC7991ECDC9BB8D7C1C4501BE1BAE9485300E

$Q_{1,2}$ = 02D0B4CC95A2DD435D0E22BFBB29C59418306F6CD00A

$Q_{2,2}$ = O45ECB881387582E7C556887784D2671CA118E22FCF2

$Q_{1,3}$ = B0C2B1F808D24F6376E3A534EB555EF54E6AEF5982

$Q_{2,3}$ = 0AB9F81DF462F58A52D937E6D81F48FFA4A87A9935AB

Q_1 = 27F7B9FC82C19ACAE47F3FE9560C3536A7E90F8C3C51E13C 35F32FD8C6823DF753685DD63555D2146FCDB9B28DA367327DD6 EDDA092D0CF108D0AB708405DA46

Q_2 = 230D0B9595E5AD388F1F447A69918905EBFB05910582E5BA64

9C94B0B2661E49DF3C9B42FEF1F37A7909B1C2DD54113ACF87C6
F11F19874DE7DC5D1DF2A9252D

Dynamic authentication

The dynamic authentication mechanism is designed to prove, to an entity known as a **controller**, the authenticity of another entity known as a **demonstrator** as well as the authenticity of a possible associated message *M*, so that the controller can be sure that it is truly the demonstrator and, as the case may be, only the demonstrator and that the demonstrator is truly speaking of the same message *M*. The associated message *M* is optional. This means that it may be vacant.

The dynamic authentication mechanism is a sequence of four acts: an act of commitment, and act of challenge, and act of response and an act of checking. The demonstrator fulfills the acts of commitment and response. The controller fulfills the acts of challenge and control.

Within the demonstrator, it is possible to isolate a witness so as to isolate the most sensitive parameters and functions of the demonstrator, namely the production of commitments and responses. The witness has the parameter k and the private key GQ2, namely the factorization of the module n according to one of the three depictions referred to here above: • the f prime factors and the m base numbers, • the $m.f$ private component, the f prime factors and the f-1 parameters of the Chinese remainders, • the m private values and the modulus n.

The witness may correspond to a partial embodiment, for example, ∝ a chip card connected to a PC forming the entire demonstrator or again, ∝ specially protected programs within a PC, or again, • specially protected programs within a smart card. The witness thus isolated is similar to the witness defined here below within the signing party. At each execution of the mechanism, the witness produces one or more commitments R and then as many responses D to as many challenges d. Each set $\{R, d, D\}$ is a **GQ2 triplet**.

Apart from comprising the witness, the demonstrator also has, if necessary, a hashing function and a message *M*.

The controller has the modulus n and the parameters k and m; if necessary, it also has the same hashing function and a message M'. The controller is capable of reconstituting a commitment R' from any challenge d and any response D. The parameters k and m inform the controller. Failing any indication to the contrary, the m base numbers from g_1 to g_m are the m first prime numbers. Each challenge d must have m elementary challenges referenced from d_1 to d_m: one per base number. This elementary challenge from d_1 to d_m may take a value of 0 to 2^{k-1}-1 (the values of $v/2$ to v-1 are not used). Typically, each challenge is encoded by m times k-1 bits (and not by m times k bits). For example, $k = 6$ and $m = 3$ and the base numbers 3, 5 and 7, each challenge has 15 bits transmitted on two bytes; with $k = 9$, $m = 2$ and the base numbers 2 and 3, each challenge has 16 bits transmitted on two bytes. When the $(k\text{-}1).m$ possible challenges are also possible, the value $(k\text{-}1).m$ determines the security provided by each GQ2 triplet: an impostor who, by definition, does not know the factorization of the module n has exactly one chance of success in $2^{(k-1).m}$. When $(k\text{-}1).m$ is equal to 15 to 20, one triplet is enough to reasonably provide for dynamic authentication. To achieve any security level, it is possible to produce triplets in parallel. It is also possible to produce sequentially, namely to repeat the execution of the mechanism.

1) The act of commitment comprises the following operations.

When the witness has m private values from Q_1 to Q_m and the modulus n, it draws one or more random values r $(0 < r < n)$ at random and privately; then by k successive squaring (mod n) operations, it converts each random value r into a commitment R.

$$R \equiv r^v \pmod n$$

Here is an example with the first set of keys with $k = 6$.

r = B8AD426C1A10165E94B894AC2437C1B1797EF562CFA53A4AF8
43131FF1C89CFDA131207194710EF9C010E8F09C60D9815121981260
919967C3E2FB4B4566088E

R = FFDD736B666F41FB771776D9D50DB7CDF03F3D976471B25C56
D3AF07BE692CB1FE4EE70FA77032BECD8411B813B4C21210C6B04

49CC4292E5DD2BDB00828AF18

When the witness has f prime factors from p_1 to p_f and $m.f$ private components Q_{ij}, it draws one or more collections of f random values at random and privately: each collection has one random value r_i per prime factor p_i ($0 < r_i < p_i$); then by k successive operations of squaring (mod p_i), it converts each random value r_i into a component of commitment R_i.

$$R_i \equiv r_i^v \pmod{p_i}$$

Here is an example with the second set of keys with $k = 9$.

r_1 = B0418EABEBADF0553A28903F74472CD49DD8C82D86

R_1 = 022B365F0BEA8E157E94A9DEB0512827FFD5149880F1

r_2 = 75A8DA8FE0E60BD55D28A218E31347732339F1D667

R_2 = 057^{E}43A242C455FC20DEEF291C774CF1B30F0163DEC2

r_3 = 0D74D2BDA5302CF8BE2F6D406249D148C6960A7D27

R_3 = 06^{E}14C8FC4DD312BA3B475F1F40CF01ACE2A88D5BB3C

For each collection of f commitment components, the witness sets up a commitment according to the technique of Chinese remainders. There are as many commitments as there are collections of random values.

$$R = \text{Chinese remainders } (R_1, R_2, \ldots, R_f)$$

R = 28AA7F12259BFBA81368EB49C93EEAB3F3EC6BF73B0EBD7
D3FC8395CFA1AD7FC0F9DAC169A4F6F1C46FB4C3458D1E37C9
9123B56446F6C928736B17B4BA4A529

In both cases, the demonstrator sends the controller all or part of each commitment ***R***, or at least a hashing code ***H*** obtained by hashing each commitment ***R*** and one message ***M***.

2) The act of challenge consists in drawing at random one or more challenges d each consisting of m elementary challenges $d_1 \mid d_2 \mid \ldots \mid d_m$; each elementary challenge d_i takes one of the values from 0 to $v/2$-1.

$$d = d_1 \mid d_2 \mid \ldots \mid d_m$$

Here is an example for the first set of keys with $k = 6$ and $m = 3$.

$d_1 = 10110 = 22 =$ '16'; $d_2 = 00111 = 7$; $d_3 = 00010 = 2$

$d = 0 \mid\mid d_1 \mid\mid d_2 \mid\mid d_3 = 01011000\ 11100010 = 58\ \text{E2}$

Here is an example for the second set of keys with $k = 9$ and $m = 2$.

$d = d_1 \,||\, d_2$ = 58 E2, that is, in decimal notation 88 and 226

The controller sends the demonstrator each challenge ***d***.

3) The act of response has the following operations.

When the witness has m private values from Q_1 to Q_m and the modulus n, it computes one or more responses D in using each random value r of the act of commitment and the private values according to the elementary challenges.

$$X \equiv Q_1^{d1}.Q_2^{d2}\ldots Q_m^{dm} (\mathrm{mod}\ n)$$

$$D \equiv r.X\ (\mathrm{mod}\ n)$$

Here is an example for the first set of keys.

D = FF257422ECD3C7A03706B9A7B28EE3FC3A4E974AEDCDF386 5EEF38760B859FDB5333E904BBDD37B097A989F69085FE8EF6480 A2C6A290273479FEC9171990A17

When the witness has f prime factors from p_i to p_f and $m.f$ private components $Q_{i,j}$, it computes one or more collections of f response components in using each collection of random values of the act of commitment: each collection of response components comprises one component per prime factor.

$$X_i \equiv Q_1^{d1}.Q_2^{d2}\ldots Q_m^{dm}{}_{,1}\ (\mathrm{mod}\ p_1)$$

$$D_i \equiv r_i.X_i\ (\mathrm{mod}\ p_1)$$

Here is an example for the second set of keys.

$D_1 = r_1.\ Q_{1.1}{}^{d1}.Q_{2.1}{}^{d2}\ (\mathrm{mod}\ p_1) =$

O2660ADF3C73B6DC15E196152322DDE8EB5B35775E38

$D_2 = r_2.\ Q_{1.2}{}^{d1}.Q_{2.2}{}^{d2}\ (\mathrm{mod}\ p_2) =$

04C15028E5FD1175724376C11BE77052205F7C62AE3B

$D_3 = r_3.\ Q_{1.3}{}^{d1}.Q_{2.3}{}^{d2}\ (\mathrm{mod}\ p_3) =$

0903D20D0C306C8EDA9D8FB5B3BEB55E061AB39CCF52

For each collection of response components, the witness draws up a response according to the Chinese remainder technique. There are as many responses as there are challenges.

D = Chinese reminders ($D_1, D_2, \ldots, D_f$)

D = 85C3B00296426E97897F73C7DC6341FB8FFE6E879AE12EF1F36
4CBB55BC44DEC437208CF530F8402BD9C511F5FB3B3A309257A00
195A7305C6FF3323F72DC1AB

In both cases, the demonstrator sends each response $\boldsymbol{D}$ to the controller.

4) The checking act consists in ascertaining that each triplet $\{R, d, D\}$ verifies an equation of the following type <u>for a non-zero value</u>,

$$R.\prod_{i=1}^{m} G_i^{d_i} \equiv D^{2^k} \pmod n \text{ or else } R \equiv D^{2^k}.\prod_{i=1}^{m} G_i^{d_i} \pmod n$$

or else in setting up each commitment: <u>none should be zero</u>.

$$R' \equiv D^{2^k} / \prod_{i=1}^{m} G_i^{d_i} \pmod n \text{ or else } R' \equiv D^{2^k}.\prod_{i=1}^{m} G_i^{d_i} \pmod n$$

If necessary, the controller then computes a hashing code H' in hashing each re-established commitment D' and a message M'. The dynamic authentication is successful when the controller thus retrieves what it had received at the end of the first act of commitment, namely all or part of each commitment R, or else the hashing code H.

For example, a sequence of elementary operations converts the response D into a commitment R'. The sequence has k squares (mod n) separated by k-1 divisions or multiplications (mod n) by base numbers. For the i-th division or multiplication, which is performed between the i-th square and the i+1st square, the i-th bit of the elementary challenge d_1 indicates that it is necessary to use g_1, the i-th bit of the elementary challenge d_2 indicates whether it is necessary to use g_2, ... up to the i-th bit of the elementary challenge d_m which indicates that it is necessary to use g_m.

Here is an example for the first set of keys.

**D^2 (mod n) = FD12E8E1F1370AEC9C7BA2E05C80AD2B692D341D46F3
2B93948715491F0EB091B7606CA1E744E0688367D7BB998F7B73D5F7
FDA95D5BD6347DC8B978CA217733**

**3 . D^2 (mod n) = F739B708911166DFE715800D8A9D78FC3F332FF622D
3EAB8E7977C68AD44962BEE4DAE3C0345D1CB34526D3B67EBE8BF
987041B4852890D83FC6B48D3EF6A9DF**

$3^2 . D^4 \pmod n$ = 682A7AF280C49FE230BEE354BF6FFB30B7519E3C8
92DD07E5A781225BBD33920E5ADABBCD7284966D71141EAA17AF
8826635790743EA7D9A15A33ACC7491D4A7

$3^4 . D^8 \pmod n$ = BE9D828989A2C184E34BA8FE0F384811642B7B548F
870699E7869F8ED851FC3DB3830B2400C516511A0C28AFDD210EC3
939E69D413F0BABC6DEC441974B1A291

$3^5 . 5 . D^8 \pmod n$ = 2B40122E225CD858B26D27B768632923F2BBE5
DB15CA9EFA77EFA667E554A02AD1A1E4F6B59BD9E1AE4A537D
4AC1E89C2235C363830EBF4DB42CEA3DA98CFE00

$3^{10} . 5^2 . D^{16} \pmod n$ = BDD3B34C90ABBC870C604E27E7F2E9DB2D383
68EA46C931C66F6C7509B118E3C162811A98169C30D4DEF768397DD
B8F6526B6714218DEB627E11FACA4B9DB268

$3^{11} . 5^3 . 7 . D^{16} \pmod n$ = DBFA7F40D338DE4FBA73D42DBF427BBF195
C13D02AB0FA5F8C8DDB5025E34282311CEF80BACDCE5D0C433444
A2AF2B15318C36FE2AE02F3C8CB25637C9AD712F

$3^{22} . 5^6 . 7^2 . D^{32} \pmod n$ = C60CA9C4A11F8AA89D9242CE717E3DC6C1
A95D5D09A2278F8FEE1DFD94EE84D09D000EA8633B53C4A0E7F0A
EECB70509667A3CB052029C94EDF27611FAE286A7

$3^{22} . 5^7 . 7^2 . D^{32} \pmod n$ = DE40CB6B41C01E722E4F312AE7205F18CDD
0303EA52261CB0EA9F0C7E0CD5EC53D42E5CB645B6BB1A3B00C77
886F4AC5222F9C863DACA440CF5F1A8E374807AC

$3^{44} . 5^{14} . 7^4 . D^{64} \pmod n$, namely $3^{2C} . 5^{E} . 7^4 . D^{40}$ with the exponents in hexadecimal notation = FFDD736B666F41FB771776D9D50DB7CDF03F3D9
76471B25C56D3AF07BE692CB1FE4EE70FA77032BECD8411B813B4C
21210C6B0449CC4292E5DD2BDB00828AF18

We find the commitment R. The authentication is successful.

Here is an example for the second set of keys.

$D^2 \pmod n$ = C66E585D8F132F7067617BC6D00BA699ABD74FB9D13E
24E6A6692CC8D2FC7B57352D66D34F5273C13F20E3FAA228D70AEC
693F8395ACEF9206B172A8A2C2CCBB

$3 . D^{2} \pmod{n}$ = 534C6114D385C3E15355233C5B00D09C2490D1B8D8E
D3D59213CB83EAD41C309A187519E5F501C4A45C37EB2FF38FBF20
1D6D138F3999FC1D06A2B2647D48283

$3^{2} . D^{4} \pmod{n}$ = A9DC8DEA867697E76B4C18527DFFC49F4658473D03
4EC1DDE0EB21F6F65978BE477C4231AC9B1EBD93D5D49422408E47
15919023B16BC3C6C46A92BBD326AADF

$2 . 3^{3} . D^{4} \pmod{n}$ = FB2D57796039DFC4AF9199CAD44B66F257A1FF
3F2BA4C12B0A8496A0148B4DFBAFE838E0B5A7D9FB4394379D72A
107E45C51FCDB7462D03A35002D29823A2BB5

$2^{2} . 3^{6} . D^{8} \pmod{n}$ = 4C210F96FF6C77541910623B1E49533206DFB9E91
6521F305F12C5DB054D4E1BF3A37FA293854DF02B49283B6DE5E5D
82ACB23DAF1A0D5A721A1890D03A00BD8

$2^{2} . 3^{7} . D^{8} \pmod{n}$ = E4632EC4FE4565FC4B3126B15ADBF996149F2D
BB42F65D911D3851910FE7EA53DAEA7EE7BA8FE9D081DB78B249
B1B18880616B90D4E280F564E49B270AE02388

$2^{4} . 3^{14} . D^{16} \pmod{n}$ = ED3DDC716AE3D1EA74C5AF935DE814BCC
2C78B12A6BB29FA542F9981C5D954F53D153B9F0198BA82690EF
665C17C399607DEA54E218C2C01A890D422EDA16FA3

$2^{5} . 3^{14} . D^{16} \pmod{n}$ = DA7C64E0E8EDBE9CF823B71AB13F17E1161487
6B000FBB473F5FCBF5A5D8D26C7B2A05D03BDDD588164E562D0F5
7AE94AE0AD3F35C61C0892F4C91DC0B08ED6F

$2^{10} . 3^{28} . D^{32} \pmod{n}$ = 6ED6AFC5A87D2DD117B0D89072C99FB9DC9
5D558F65B6A1967E6207D4ADBBA32001D3828A35069B256A07C3D
722F17DA30088E6E739FBC419FD7282D16CD6542

$2^{11} . 3^{28} . D^{32} \pmod{n}$ = DDAD5F8B50FA5BA22F61B120E5933F73B92
BAAB1ECB6D432CFCC40FA95B77464003A705146A0D364AD40F8
7AE45E2FB460111CDCE73F78833FAE505A2D9ACA84

$2^{22} . 3^{56} . D^{64} \pmod{n}$ = A466D0CB17614EFD961000BD9EABF4F021
36F8307101882BC1764DBAACB715EFBF5D8309AE001EB5DEDA
8F000E44B3D4578E5CA55797FD4BD1F8E919BE787BD0

$2^{44} . 3^{112} . D^{128} \pmod{n}$ = 925B0EDF5047EFEC5AFABDC03A830919761

B8FBDD2BF934E2A8A31E29B976274D513007EF1269E4638B4F65F 8FDEC740778BDC178AD7AF2968689B930D5A2359

$2^{44} . 3^{113} . D^{128} \pmod n$ = B711D89C03FDEA8D1F889134A4F809B3F2D 8207F2AD8213D169F2E99ECEC4FE08038900F0C203B55EE4F4C803 BFB912A04F11D9DB9D076021764BC4F57D47834

$2^{88} . 3^{226} . D^{256} \pmod n$ = 41A83F119FFE4A2F4AC7E5597A5D0BEB4D4C 08D19E597FD034FE720235894363A19D6BC5AF323D24B1B7FCFD8D FCC628021B4648D7EF757A3E461EF0CFF0EA13

$2^{176} . 3^{452} . D^{512} \pmod n$ that is $4^{88} . 9^{226} . D^{512} \pmod n$ = 28AA7F12259BFBA8 1368EB49C93EEAB3F3EC6BF73B0EBD7D3FC8395CFA1AD7FC0F9D AC169A4F6F1C46FB4C3458D1E37C99123B56446F6C928736B17B4BA 4A529

We find the commitment ***R***. The authentication is successful.

Digital signature

The digital signing mechanism enables an entity called a **signing party** to produce signed messages and an entity called a **controller** to ascertain signed messages. The message *M* is any binary sequence: it may be vacant. The message *M* is signed by adding a signature appendix to it. This signature appendix comprises one or more commitments and/or challenges as well as the corresponding responses.

The controller has the same hashing function, the parameters k and m and the module n. The parameters $\boldsymbol{k}$ and $\boldsymbol{m}$ provide information to the controller. Firstly, each elementary challenge from d_1 to d_m must take a value from 0 to 2_{k-1}-1 (the values of $v/2$ to v-1 are not used). Secondly, each challenge d must comprise m elementary challenges referenced from d_1 to d_m, namely as many of them as base numbers. Furthermore, failing indications to the contrary, the m base numbers from g_1 to g_m are the m first prime numbers. With $(k-1).m$ equal to 15 to 20, it is possible to sign with four triplets GQ2 produced in parallel; with $(k-1).m$ equal to 60 or more, it is possible to sign with a single triplet GQ2. For example, with $k = 9$ and $m = 8$, a single triplet GQ2 is enough; each challenge has eight bytes and the base numbers are 2, 3, 5, 7, 11, 13, 17 and 19.

The signing operation is a sequence of three acts: an act of commitment, an act of challenge and an act of response. Each act produces one or more GQ2 triplets each comprising: a commitment R ($\neq 0$), a challenge d consisting of m elementary challenges referenced $d_1, d_2, \ldots, d_m$ and a response D ($\neq 0$).

The signing party has a hashing function, the parameter k and the GQ2 private key, namely the factorization of the modulus n according to one of the three depictions referred to here above. **Within the signing party, it is possible to isolate a witness that performs the the acts of commitment and response**, so as to isolate the functions and parameters most sensitive to the demonstrator. To compute commitments and responses, the witness has the parameter k and the GQ2 private key, namely the factorization of the modulus n according to one of the three depictions referred to here above. The witness thus isolated is similar to the witness defined within the demonstrator. It may correspond to a particular embodiment, for example, $\propto$ a chip card connected to a PC forming the entire signing party, or again, $\propto$ programs particularly protected within a PC, or again, $\propto$ programs particularly protected within a chip card.

1) The act of commitment comprises the following operations:

When the witness has m private values from Q_1 to Q_m and the modulus n, it randomly and privately draws one or more random values r ($0 < r < n$); then, by k successful squaring (mod n) operations, it converts each random value r into a commitment R.

$$R_i \equiv r^v \pmod{n}$$

When the witness has f prime factors from p_1 to p_f and $m.f$ private components Q_{ij}, it privately and randomly draws one or more collections of f random values: each collection has one random value r_i per prime factor p_i ($0 < r_i < p_i$); then, by k successive squaring (mod p_i) operations, it converts each random value r_i into a component of commitment R_i.

$$R_i \equiv r_i^v \pmod{p_i}$$

For each collection of f commitment components, the witness sets up a commitment according to the Chinese remainder technique. There are as many commitments as there are collections of random values.

$$R = \text{Chinese remainders } (R_1, R_2, \ldots, R_f)$$

2) The act of challenge consists in hashing all the commitments R and the message to be signed M to obtain a hashing code from which the signing party forms one or more challenges each comprising m elementary challenges; each elementary challenge takes a value from 0 to $v/2$-1; for example with $k = 9$ and $m = 8$. Each challenge has eight bytes. There are as many challenges as there are commitments.

$$d = d_1 \mid d_2 \mid \ldots \mid d_m, \text{ extracted from the result Hash}(M, R)$$

3) The act of response comprises the following operations.

When the witness has m private values from Q_1 to Q_m and the modulus n, it computes one or more responses D using each random value r of the act of commitment and the private values according to the elementary challenges.

$$X. / \equiv Q_1^{d1}.Q_2^{d2}\ldots Q_m^{dm} \pmod n$$

$$D / \equiv r. /X. / \pmod n$$

When the witness has f prime factors from p_1 to p_f and $m.f$ private components Q_{ij}, it computes one or more collections of f response components in using each collection of random values of the act of commitment : each collection of response components comprises one component per prime factor.

$$X_i \equiv Q_1^{d1}{}_{,i}.\ Q_2^{d2}{}_{,i} \ldots Q_m^{dm}{}_{,i} \pmod{p_i}$$

$$D_i \equiv r_i.X_i \pmod{p_i}$$

For each collection of response components, the witness sets up a response according to the Chinese remainders technique. There are as many responses as there are challenges.

$$D = \text{Chinese remainders } (D_1, D_2, \ldots, D_f)$$

The signing party signs the message *M* in adding to it a signature appendix comprising:

- either each GQ2 triplet, namely each commitment R, each challenge d and each response D,

- or else each commitment R and each corresponding response D,
- or else each challenge d and each corresponding response D.

The running of the verification operation depends on the contents of the signature appendix. There are three possible cases.

Should the appendix comprise one or more triplets, the checking operation has two independent processes for which the chronology is not important. The controller accepts the signed message if and only if the two following conditions are fulfilled.

Firstly, each triplet must be consistent (an appropriate relationship for the following type has to be verified) and acceptable (the comparison has to be done on a non-zero value).

$$R.\prod_{i=1}^{m} G_i^{d_i} \equiv D^{2^k} \pmod n \text{ or else } R \equiv D^{2^k}.\prod_{i=1}^{m} G_i^{d_i} \pmod n$$

For example, the response D is converted by a sequence of elementary operations: k squared (mod n) separated by k-1 multiplication or division operations (mod n) by base numbers. For the i-th multiplication or division which is performed between the i-th square and the i+1st square, the i-th bit of the elementary challenge d_1 indicates whether it is necessary to use g_1, the i-th bit of the elementary challenge d_2 indicates whether it is necessary to use g_2, ... up to the i-th bit of the elementary challenge d_m which indicates if it is necessary to use g_m. It is thus necessary to retrieve each commitment R present in the signature appendix.

Furthermore, the triplet or triplets must be linked to the message M. By hashing all the commitments R and the message M, a hashing code is obtained from which each challenge d must be recovered.

$d = d_1 \mid d_2 \mid \ldots \mid d_m$, identical to those extracted from the result Hash(M, R)

Should the appendix have no challenge, the checking operation starts with a reconstruction of one or more challenges d' by hashing all the commitments R and the message M.

$D' = d'_1 \mid d'_2 \mid \ldots \mid d'_m$, extracted from the result Hash(M, R)

Then, the controller accepts the signed message if and only if each triplet is consistent (an appropriate relationship of the following type is verified) and acceptable (the comparison is done on a non-zero value).

$$R.\prod_{i=1}^{m} G_i^{d_i} \equiv D^{2^k} \pmod{n} \text{ or else } R \equiv D^{2^k}.\prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

Should the appendix comprise no commitment, the checking operation starts by reconstructing one or more commitments R' according to one of the following two formulae, namely the one that is appropriate. No re-established commitment should be zero.

$$R' \equiv D^{2^k} / \prod_{i=1}^{m} G_i^{d_i} \pmod{n} \text{ or else } R' \equiv D^{2^k}.\prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

Then, the controller must hash all the commitments R' and the message M so as to reconstitute each challenge d.

$d = d_1 \mid d_2 \mid \ldots \mid d_m$, identical to those extracted from the result Hash(M, R)

The controller accepts the signed message if and only if each reconstituted challenge is identical to the corresponding challenge in the appendix.

In the present application, it has been shown that there are pairs of private values and public values Q and G respectively used to implement the method, system and device according to the invention, designed to prove the authenticity of an entity and/or integrity and/or authenticity of a message.

In the pending application filed on the same day as the present application by France Télécom, TDF and the firm Math RiZK, whose inventors are Louis Guillou and Jean-Jacques Quisquater, a method has been described for the production of sets of GQ2 keys namely moduli n and pairs of public and private values G and Q respectively when the exponent v is equal to 2^k. This patent application is incorporated herein by reference.

CLAIMS

1. Method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the following parameters or derivatives of these parameters:

- **m** pairs of private values $\mathbf{Q_1, Q_2, \ldots Q_m}$ and public values $\mathbf{G_1, G_2, \ldots G_m}$ (**m** being greater than or equal to 1),
- a public modulus **n** constituted by the product of f prime factors $\mathbf{p_1, p_2, \ldots p_f}$ (**f** being greater than or equal to 2),
- a public exponent **v**;

said modulus, said exponent and said values being related by relations of the following type

$$G_i \, . \, Q_i^v \equiv 1 \, . \bmod n \text{ or } G_i \equiv Q_i^v \bmod n;$$

said exponent **v** being such that

$$v = 2^k$$

where **k** is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the **f** prime factors $\mathbf{p_1, p_2, \ldots p_f}$, the base number g_i being such that:

the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \qquad x^2 \equiv - g_i \bmod n$$

cannot be resolved in x in the ring of integers modulo **n**

and such that:

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n**;

said method implements, in the following steps, an entity called a witness having **f** prime factors p_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or the **f.m**

components $\mathbf{Q}_{i,\,j}$ ($\mathbf{Q}_{i,\,j} \equiv \mathbf{Q}_i \bmod \mathbf{p}_j$) of the private values $\mathbf{Q}_i$ and of the public exponent **v**;

- the witness computes commitments **R** in the ring of integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R} \equiv \mathbf{r}^{\mathbf{v}} \bmod \mathbf{n}$$

where **r** is a random value such that $\mathbf{0} < \mathbf{r} < \mathbf{n}$,

• or

• • by performing operations of the type:

$$\mathbf{R}_i \equiv \mathbf{r}_i^{\mathbf{v}} \bmod \mathbf{p}_i$$

where $\mathbf{r}_i$ is a random value associated with the prime number $\mathbf{p}_i$ such that $\mathbf{0} < \mathbf{r}_i < \mathbf{p}_i$, each $\mathbf{r}_i$ belonging to a collection of random values $\{\mathbf{r}_1, \mathbf{r}_2, \ldots \mathbf{r}_f\}$,

• • then by applying the Chinese remainder method;

- the witness receives one or more challenges **d**, each challenge **d** comprising **m** integers $\mathbf{d}_i$ hereinafter called elementary challenges; the witness, on the basis of each challenge **d**, computes a response **D**,

• either by performing operations of the type:

$$\mathbf{D} \equiv \cdot\cdot\, .\, \mathbf{Q}_1^{\,\mathbf{d1}} \,.\, \mathbf{Q}_2^{\,\mathbf{d2}} . \ldots \mathbf{Q}_m^{\,\mathbf{dm}} \bmod \mathbf{n}$$

• or

• • by performing operations of the type:

$$\mathbf{D}_i \equiv \mathbf{r}_i \,.\, \mathbf{Q}_{i,1}^{\,\mathbf{d1}} \,.\, \mathbf{Q}_{i,2}^{\,\mathbf{d2}} . \ldots \mathbf{Q}_{i,m}^{\,\mathbf{dm}} \bmod \mathbf{p}_i$$

• • and then by applying the Chinese remainder method;

said method being such that there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}**.

2. Method according to claim 1, designed to prove the authenticity of an entity known as a demonstrator to an entity known as the controller, said demonstrator entity comprising the witness;

said demonstrator and controller entities executing the following steps:

• **Step 1: act of commitment R**

- at each call, the witness computes each commitment **R** by applying the process specified according to claim 1,

- the demonstrator sending the controller all or part of each commitment **R**,

• **Step 2: act of challenge d**

- the controller, after having received all or part of each commitment **R**, produces challenges **d** whose number is equal to the number of commitments **R** and sends the challenges **d** to the demonstrator,

• **Step 3: act of response D**

- the witness computes the responses **D** from the challenges **d** by applying the process specified in claim 1,

• **Step 4: act of checking**

- the demonstrator sends each response **D** to the controller,

case where the demonstrator has transmitted a part of each commitment R

if the demonstrator has transmitted a part of each commitment **R**, the controller, having the **m** public values $G_1, G_2, \ldots, G_m$, computes a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

or a relationship of the type

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

the controller ascertains that each reconstructed commitment **R'** reproduces all or part of each commitment **R** that has been transmitted to it.

Case where the demonstrator has transmitted the totality of each commitment R

if the demonstrator has transmitted the totality of each commitment **R**, the controller, having the **m** public values $G_1, G_2, \ldots, G_m$, ascertains that each commitment **R** satisfies a relationship of the type

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

or a relationship of the type

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

3. Method according to claim 1, designed to provide proof to an entity, known as the controller entity, of the integrity of a message **M** associated with an entity called a demonstrator entity, said demonstrator entity comprising the witness; said demonstrator and controller entities executing the following steps:

• **Step 1: act of commitment R**

- at each call, the witness computes each commitment **R** by applying the process specified according to claim 1,

• **Step 2: act of challenge d**

- the demonstrator applies a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute at least one token **T,**

- the demonstrator sends the token **T** to the controller,

- the controller, after having received a token **T**, produces challenges **d** equal in number to the number of commitments **R** and sends the challenges **d** to the demonstrator,

• **Step 3: act of response D**

- the witness computes the responses **D** from the challenges **d** by applying the process specified according to claim 1,

• **Step 4: act of checking**

- the demonstrator sends each response **D** to the controller,

- the controller, having the **m** public values G_1, G_2, ..., G_m, computes a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

or a relationship of the type

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

- then the controller applies the hashing function **h** whose arguments are the message **M** and all or part of each reconstructed commitment **R'** to reconstruct the token **T'**,

- then the controller ascertains that the token **T'** is identical to the token **T** transmitted.

4. Method according to claim 1, designed to produce the digital signature of a message **M** by an entity known as the signing entity, said signing entity comprising the witness;

Signing operation

said signing entity executes a signing operation in order to obtain a signed message comprising:

- the message **M**,
- the challenges **d** and/or the commitments **R**,
- the responses **D**;

said signing entity executes the signing operation by implementing the following steps:

• **Step 1: act of commitment R**

- at each call, the witness computes each commitment **R** by applying the process specified according to claim 1,

• **Step 2: act of challenge d**

- the signing party applies a hashing function **h** whose arguments are the message **M** and each commitment **R** to obtain a binary train,
- from this binary train, the signing party extracts challenges **d** whose number is equal to the number of commitments **R**,

• **Step 3: act of response D**

- the witness computes the responses **D** from the challenges **d** by applying the process specified according to claim 1.

5. Method according to claim 4, designed to prove the authenticity of the message M by checking the signed message through an entity called a controller;

Checking operation

- said controller entity having the signed message executes a checking operation by proceeding as follows:

• **case where the controller has commitments R, challenges d, responses D**

if the controller has commitments **R**, challenges **d**, responses **D**,

• • the controller ascertains that the commitments **R**, the challenges **d** and the responses **D** satisfy relationships of the type

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

or relationships of the type:

$$R \equiv D^v/G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

• • the controller ascertains that the message **M**, the challenges **d** and the commitments **R** satisfy the hashing function:

$$d = h\ (\text{message}, R)$$

• **case where the controller has challenges d and responses D**

if the controller has challenges **d** and responses **D**,

• • the controller reconstructs, on the basis of each challenge **d** and each response **D**, commitments **R'** satisfying relationships of the type

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

or relationships of the type:

$$R' \equiv D^v/G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

• • the controller ascertains that the message **M** and the challenges **d** satisfy the hashing function:

$$d = h\ (\text{message}, R')$$

• **case where the controller has commitments R and responses D**

if the controller has commitments **R** and responses **D**,

• • the controller applies the hashing function and reconstructs **d'**

$$d' = h\ (\text{message}, R)$$

• • the controller device ascertains that the commitments **R**, the challenges **d'** and the responses **D** satisfy relationships of the type

$$R \equiv G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . D^v \bmod n$$

or relationships of the type:

$$R \equiv D^v/G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . \bmod n$$

6. A system designed to prove, to a controller server,

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity,

by means of all or part of the following parameters or derivatives of these parameters:

- **m** pairs of private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$ (**m** being greater than or equal to 1),

- a public modulus **n** constituted by the product of said **f** prime factors $p_1, p_2, \ldots p_f$ (**f** being greater than or equal to 2),

- a public exponent **v**.

said modulus, said exponent and said values being linked by relations of the type

$$G_i . Q_i^v \equiv 1 . \bmod n \text{ or } G_i \equiv Q_i^v \bmod n .$$

said exponent **v** is such that

$$v = 2^k$$

where **k** is a security parameter greater than 1;

said public value G_i being the square g_i^2 of the base number g_i smaller than the **f** prime factors $p_1, p_2, \ldots p_f$, the base number g_i being such that:

the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv - g_i \bmod n$$

cannot be resolved in x in the ring of integers modulo **n**

and such that:

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n**;

said system comprises a witness device, contained especially in a nomad object which, for example, takes the form of a microprocessor-based bank card,

the witness device comprises

- a memory zone containing the **f** prime factors p_i and/or the parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values Q_i and/or **f.m** components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent **v** ;

said witness device also comprises:

- random value production means, hereinafter called random value production means of the witness device,

- computation means, hereinafter called means for the computation of commitments **R** of the witness device, to compute commitments **R** in the ring of integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R} \equiv \mathbf{r}^{v} \bmod \mathbf{n}$$

where **r** is a random value produced by the random value production means, r being such that $\mathbf{0} < \mathbf{r} < \mathbf{n}$,

• or by performing operations of the type:

$$\mathbf{R_i} \equiv \mathbf{r_i}^{v} \bmod \mathbf{p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0} < \mathbf{r_i} < \mathbf{p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\{\mathbf{r_1}, \mathbf{r_2}, \ldots \mathbf{r_f}\}$, then by applying the Chinese remainder method;

said witness device also comprises:

- reception means hereinafter called the means for the reception of the challenges **d** of the witness device, to receive one or more challenges **d**; each challenge **d** comprising **m** integers $\mathbf{d_i}$ hereinafter called elementary challenges;

- computation means, hereinafter called means for the computation of the responses **D** of the witness device for the computation, on the basis of each challenge **d, of** a response **D**,

• either by performing operations of the type:

$$\mathbf{D} \equiv \mathbf{r} \cdot \mathbf{Q_1}^{\mathbf{d1}} \cdot \mathbf{Q_2}^{\mathbf{d2}} \cdot \ldots \mathbf{Q_m}^{\mathbf{dm}} \bmod \mathbf{n}$$

• or by performing operations of the type:

$$\mathbf{D_i} \equiv \mathbf{r_i} \cdot \mathbf{Q_{i,1}}^{\mathbf{d1}} \cdot \mathbf{Q_{i,2}}^{\mathbf{d2}} \cdot \ldots \mathbf{Q_{i,m}}^{\mathbf{dm}} \bmod \mathbf{p_i}$$

and then by applying the Chinese remainder method.

- transmission means to transmit one or more commitments **R** and one or more responses **D;**

there are as many responses **D** as there are challenges **d** as there are commitments **R,** each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}.**

7. A system according to claim 6, designed to prove the authenticity of an entity called a demonstrator and an entity called a controller,
said system being such that it comprises:

- a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

- a controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device;

said system enabling the execution of the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified according to claim 1, the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,
the demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator, to transmit all or part of each commitment **R** to the controller device through the connection means;

• **Step 2: act of challenge d**

the controller device comprises challenge production means for the production, after receiving all or part of each commitment **R**, of the challenges **d** equal in number to the number of commitments **R**,
the controller device also has transmission means, hereinafter known as the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means ;

• **Step 3: act of response D**

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the demonstrator device through the interconnection means,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified according to claim 1,

• **Step 4: act of checking**

the transmission means of the demonstrator transmit each response **D** to the controller,

the controller device also comprises:

- computation means, hereinafter called the computation means of the controller device,

- comparison means, hereinafter called the comparison means of the controller device,

case where the demonstrator has transmitted a part of each commitment R.

if the transmission means of the demonstrator have transmitted a part of each commitment **R**, the computation means of the controller device, having **m** public values $\mathbf{G_1, G_2, \ldots, G_m}$, compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$\mathbf{R' \equiv G_1{}^{d1} . G_2{}^{d2} . \ldots G_m{}^{dm} . D^v \bmod n}$$

or a relationship of the type

$$\mathbf{R' \equiv D^v / G_1{}^{d1} . G_2{}^{d2} . \ldots G_m{}^{dm} . \bmod n}$$

the comparison means of the controller device compare each reconstructed commitment **R'** with all or part of each commitment **R** received,

case where the demonstrator has transmitted the totality of each commitment R

if the transmission means of the demonstrator have transmitted the totality of each commitment **R**, the computation means and the comparison means of the controller

device, having **m** public values $G_1, G_2, ..., G_m$, ascertain that each commitment **R** satisfies a relationship of the type

$$R \equiv G_1^{d1} . G_2^{d2} . ... G_m^{dm} . D^v \bmod n$$

or a relationship of the type

$$R \equiv D^v/G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \bmod n$$

8. System according to claim 6, designed to give proof to an entity, known as a controller, of the integrity of a message **M** associated with an entity known as a demonstrator,

said system being such that it comprises

- a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

- a controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device;

said system enabling the execution of the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified in claim 1

the witness device has transmission means, hereinafter called transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

• **Step 2: act of challenge d**

the demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function **h** whose

arguments are the message **M** and all or part of each commitment **R** to compute at least one token **T**,

the demonstrator device also has transmission means, hereinafter known as the transmission means of the demonstrator device, to transmit each token **T** through the connection means to the controller device,

the controller device also has challenge production means for the production, after having received the token **T**, of the challenges **d** in a number equal to the number of commitments **R**,

the controller device also has transmission means, hereinafter called the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means;

• **Step 3: act of response D**

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the demonstrator device through the interconnection means,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified according to claim 1,

• **Step 4: act of checking**

the transmission means of the demonstrator transmit each response **D** to the controller,

the controller device also comprises computation means, hereinafter called the computation means of the controller device, having **m** public values $G_1, G_2, \ldots, G_m$, to firstly compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

or a relationship of the type

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n$$

then, secondly, compute a token **T'** by applying the hashing function **h** having as arguments the message **M** and all or part of each reconstructed commitment **R'**,

the controller device also has comparison means, hereinafter known as the comparison means of the controller device, to compare the computed token **T'** with the received token **T**.

9. System according to claim 6, designed to produce the digital signature of a message **M**, hereinafter known as the signed message, by an entity called a signing entity;

the signed message comprising:

- the message **M**,
- the challenges **d** and/or the commitments **R**,
- the responses **D**;

Signing operation

said system being such that it comprises a signing device associated with the signing entity, said signing device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said system enabling the execution of the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified according to claim 1, the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

• **Step 2: act of challenge d**

the signing device comprises computation means, hereinafter called the computation means of the signing device, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute a binary train and extract, from this binary train, challenges **d** whose number is equal to the number of commitments **R**,

• **Step 3: act of response D**

the means for the reception of the challenges **d** of the witness device receive each challenge **d** coming from the signing device through the interconnection means,
the means for computing the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified according to claim 1,
the witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses **D** to the signing device through the interconnection means.

10. System according to claim 9, designed to prove the authenticity of the message **M** by checking the signed message by means of an entity called the controller;

Checking operation

the system being such that it comprises a controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server, said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the signing device;
the signing device associated with the signing entity comprises transmission means, hereinafter known as the transmission means of the signing device, for the transmission, to the controller device, of the signed message through the connection means, in such a way that the controller device has a signed message comprising:

- the message **M**,
- the challenges **d** and/or the commitments **R**,
- the responses **D**;

the controller device comprises:

- computation means hereinafter called the computation means of the controller device,
- comparison means, hereinafter called the comparison means of the controller device,

• case where the controller device has commitments R, challenges d, responses D

if the controller has commitments **R**, challenges **d**, responses **D**,

• • the computation and comparison means of the controller device ascertain that the commitments **R**, the challenges **d** and the responses **D** satisfy relationships of the type

$$\mathbf{R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n}$$

or relationships of the type:

$$\mathbf{R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n}$$

• • the computation and comparison means of the controller device ascertain that the message **M**, the challenges **d** and the commitments **R** satisfy the hashing function:

$$\mathbf{d = h\ (message, R)}$$

• case where the controller device has challenges d and responses D

if the controller device has challenges **d** and responses **D**,

• • the computation means of the controller, on the basis of each challenge **d** and each response **D,** compute commitments **R'** satisfying relationships of the type

$$\mathbf{R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n}$$

or relationships of the type:

$$\mathbf{R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \bmod n}$$

• • the computation and comparison means of the controller device ascertain that the message **M** and the challenges **d** satisfy the hashing function:

$$\mathbf{d = h\ (message, R')}$$

• case where the controller device has commitments R and responses D

if the controller device has commitments **R** and responses **D,**

• • the computation means of the controller device apply the hashing function and compute **d'** such that

$$\mathbf{d' = h\ (message, R)}$$

• • the computation and comparison means of the controller device ascertain that the commitments **R,** the challenges **d'** and the responses **D** satisfy relationships of the type

$$\mathbf{R \equiv G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . D^v \bmod n}$$

or relationships of the type:

$$R \equiv D^v / G_1^{d'1} \,.\, G_2^{d'2} \,.\, ... \, G_m^{d'm} \,.\, \bmod n$$

11. A terminal device associated with an entity, taking the form especially of a nomad object, for example the form of a microprocessor in a microprocessor-based bank card, designed to prove to a controller server:

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity;

by means of all or part of the following parameters or derivatives of these parameters:

- **m** pairs of private values $Q_1, Q_2, \ldots Q_m$ and public values $G_1, G_2, \ldots G_m$ (**m** being greater than or equal to 1),
- a public modulus **n** constituted by the product of said **f** prime factors $p_1, p_2, \ldots p_f$ (**f** being greater than or equal to 2),
- a public exponent **v**.

said modulus, said exponent and said values being related by relations of the type

$$G_i \,.\, Q_i^v \equiv 1 \,.\, \bmod n \text{ or } G_i \equiv Q_i^v \bmod n \,.$$

said exponent **v** being such that

$$v = 2^k$$

where **k** is a security parameter greater than 1.

said public value G_i being the square g_i^2 of the base number g_i smaller than the **f** prime factors $p_1, p_2, \ldots p_f$, the base number g_i being such that:

the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \quad x^2 \equiv - g_i \bmod n$$

cannot be resolved in x in the ring of integers modulo **n**

and such that

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n.**

said terminal device comprises a witness device comprising,

- a memory zone containing the **f** prime factors $\mathbf{p_i}$ and/or the parameters of the Chinese remainders of the prime factors and/or the public modulus **n** and/or the **m** private values $\mathbf{Q_i}$ and/or **f.m** components $\mathbf{Q_{i,j}}$ ($\mathbf{Q_{i,j} \equiv Q_i \bmod p_j}$) of the private values $\mathbf{Q_i}$ and of the public exponent **v**.

said witness device also comprises:

- random value production means, hereinafter called random value production means of the witness device,

- computation means, hereinafter called means for the computation of commitments **R** of the witness device, to compute commitments **R** in the ring of the integers modulo **n**; each commitment being computed:

• either by performing operations of the type:

$$\mathbf{R \equiv r^v \bmod n}$$

where **r** is a random value produced by the random value production means, r being such that $\mathbf{0 < r < n}$,

• or by performing operations of the type:

$$\mathbf{R_i \equiv r_i^v \bmod p_i}$$

where $\mathbf{r_i}$ is a random value associated with the prime number $\mathbf{p_i}$ such that $\mathbf{0 < r_i < p_i}$, each $\mathbf{r_i}$ belonging to a collection of random values $\mathbf{\{r_1 , r_2 , \ldots r_f\}}$ produced by the random value production means, then by applying the Chinese remainder method;

the witness device also comprises:

- reception means hereinafter called the means for the reception of the challenges **d** of the witness device, to receive one or more challenges **d**; each challenge **d** comprising **m** integers $\mathbf{d_i}$ hereinafter called elementary challenges;

- computation means, hereinafter called means for the computation of the responses **D** of the witness device, for the computation, on the basis of each challenge **d, of** a response **D**,

• either by performing operations of the type:

$$\mathbf{D \equiv r \cdot Q_1^{\,d1} \cdot Q_2^{\,d2} \cdot \ldots Q_m^{\,dm} \bmod n}$$

• or by performing operations of the type:

$$\mathbf{D_i \equiv r_i \cdot Q_{i,1}^{\,d1} \cdot Q_{i,2}^{\,d2} \cdot \ldots Q_{i,m}^{\,dm} \bmod p_i}$$

and then by applying the Chinese remainder method,

- transmission means to transmit one or more commitments **R** and one or more responses **D** ;

there are as many responses **D** as there are challenges **d** as there are commitments **R**, each group of numbers **R, d, D** forming a triplet referenced **{R, d, D}.**

12. A terminal device according to claim 11, designed to prove the authenticity of an entity called a demonstrator to an entity called a controller.

said terminal device being such that it comprises a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and being capable especially of taking the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said demonstrator device also comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

said terminal device enabling the execution of the following steps:

• Step 1: act of commitment R

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified according to claim 1, the witness device has transmission means, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

the demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator, to transmit all or part of each commitment **R** to the controller device, through the connection means;

• Steps 2 and 3: act of challenge d, act of response D

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the controller device through the connection means

between the controller device and the demonstrator device and through the interconnection means between the demonstrator device and the witness device, the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified according to claim 1,

• **Step 4: act of checking**

the transmission means of the demonstrator transmit each response **D** to the controller that carries out the check.

13. Terminal device according to claim 11, designed to give proof to an entity, known as a controller, of the integrity of a message **M** associated with an entity known as a demonstrator,

said terminal device being such that it comprises a demonstrator device associated with the demonstrator entity, said demonstrator device being interconnected with the witness device by interconnection means and being capable especially of taking the form of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said demonstrator device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

said terminal device being used to execute the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified according to claim 1; the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the demonstrator device through the interconnection means,

• **Steps 2 and 3: act of challenge d, act of response D**

the demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute at least one token **T**,

the demonstrator device also has transmission means, hereinafter known as the transmission means of the demonstrator device, to transmit each token **T,** through the connection means, to the controller device,

*(said controller, after having received the token **T**, produces challenges **d** in a number equal to the number of commitments **R**,)*

the means of reception of the challenges **d** of the witness device receive each challenge **d** coming from the controller device through the connection means between the controller device and the demonstrator device and through the interconnection means between the demonstrator device and the witness device,

the means of computation of the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified according to claim 1,

• **Step 4: act of checking**

the transmission means of the demonstrator send each response **D** to the controller device which performs the check.

14. Terminal device according to claim 11, designed to produce the digital signature of a message **M**, hereinafter known as the signed message, by an entity called a signing entity;

the signed message comprising:

- the message **M,**
- the challenges **d** and/or the commitments **R**,
- the responses **D**;

said terminal device being such that it comprises a signing device associated with the signing entity, said signing device being interconnected with the witness device by interconnection means and possibly taking especially the form of logic microcircuits

in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

said demonstrator device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the controller device associated with the controller entity, said controller device especially taking the form of a terminal or remote server;

Signing operation

said terminal device being used to execute the following steps:

• **Step 1: act of commitment R**

at each call, the means of computation of the commitments **R** of the witness device compute each commitment **R** by applying the process specified according to claim 1, the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment **R** to the signing device through the interconnection means,

• **Step 2: act of challenge d**

the signing device comprises computation means, hereinafter called the computation means of the signing device, applying a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute a binary train and extract, from this binary train, challenges **d** whose number is equal to the number of commitments **R**,

• **Step 3: act of response D**

the means for the reception of the challenges **d** of the witness device receive each challenge **d** coming from the signing device through the interconnection means,

the means for computing the responses **D** of the witness device compute the responses **D** from the challenges **d** by applying the process specified according to claim 1,

the witness device comprises transmission means, hereinafter called means of transmission of the witness device, to transmit the responses **D** to the signing device, through the interconnection means.

15. Controller device especially taking the form of a terminal or remote server associated with a controller entity, designed to check:

- the authenticity of an entity and/or
- the integrity of a message **M** associated with this entity

by means of all or part of the following parameters or derivatives of these parameters:

- **m** pairs of public values $G_1, G_2, \dots G_m$ (**m** being greater than or equal to 1),
- a public modulus **n** constituted by the product of said **f** prime factors $p_1, p_2, \dots p_f$ (**f** being greater than or equal to 2), unknown to the controller device and to the associated controller entity,
- a public exponent **v**;

said modulus, said exponent and said values being related by relations of the type

$$G_i \cdot Q_i^v \equiv 1 \cdot \bmod n \text{ or } G_i \equiv Q_i^v \bmod n \ .$$

where Q_i designates a private value, unknown to the controller device, associated with the public value G_i.

said exponent **v** being such that

$$v = 2^k$$

where **k** is a security parameter greater than 1;

said public value G_i being the square g_i^2 of a base number g_i smaller than the **f** prime factors $p_1, p_2, \dots p_f$, the base number g_i being such that

the two equations:

$$x^2 \equiv g_i \bmod n \quad \text{and} \qquad x^2 \equiv - g_i \bmod n$$

cannot be resolved in x in the ring of integers modulo **n** and such that:

the equation:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of the integers modulo **n**.

16. Controller device according to claim 15, designed to prove the authenticity of an entity called a demonstrator to an entity called a controller;

said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing

communications network, to a demonstrator device associated with the demonstrator entity;

sid controller device being used to execute the following steps:

• Steps 1 and 2: act of commitment R, act of challenge d

said controller device also has means for the reception of all or part of the commitments **R** coming from the demonstrator device through the connection means, the controller device has challenge production means for the production, after receiving all or part of each commitment **R**, of the challenges **d** in a number equal to the number of commitments **R**, each challenge **d** comprising **m** integers $\mathbf{d_i}$ hereinafter called elementary challenges.

the controller device also has transmission means, hereinafter called transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means;

• Steps 3 and 4: act of response D, act of checking

said controller device also comprises:

- means for the reception of the responses D coming from the demonstrator device, through the connection means,

- computation means, hereinafter called the computation means of the controller device,

- comparison means, hereinafter called the comparison means of the controller device,

case where the demonstrator has transmitted a part of each commitment R.

if the reception means of the demonstrator have received a part of each commitment **R**, the computation means of the controller device, having **m** public values $\mathbf{G_1}$, $\mathbf{G_2}$, ..., $\mathbf{G_m}$, compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$\mathbf{R' \equiv G_1{}^{d1} . G_2{}^{d2} . ... G_m{}^{dm} . D^v \bmod n}$$

or a relationship of the type

$$\mathbf{R' \equiv D^v / G_1{}^{d1} . G_2{}^{d2} . ... G_m{}^{dm} . \bmod n}$$

the comparison means of the controller device compare each reconstructed commitment **R'** with all or part of each commitment **R** received,

case where the demonstrator has transmitted the totality of each commitment R

if the transmission means of the demonstrator have received the totality of each commitment **R**, the computation means and the comparison means of the controller device, having **m** public values $G_1, G_2, ..., G_m$, ascertain that each commitment **R** satisfies a relationship of the type

$$R \equiv G_1^{d1} . G_2^{d2} . ... G_m^{dm} . D^v \bmod n$$

or a relationship of the type

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \bmod n$$

17. Controller device according to claim 15, designed to give proof to an entity, known as a controller, of the integrity of a message **M** associated with an entity known as a demonstrator,

said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to a demonstrator device associated with the demonstrator entity,

said system enabling the execution of the following steps:

• **Steps 1 and 2: act of commitment R, act of challenge d**

said controller device also has means for the reception of tokens **T** coming from the demonstrator device through the connection means,

the controller device has challenge production means for the production, after having received the token **T**, of the challenges **d** in a number equal to the number of commitments **R**, each challenge **d** comprising **m** integers d_i, herein after called elementary challenges,

the controller device also has transmission means, hereinafter called the transmission means of the controller, to transmit the challenges **d** to the demonstrator through the connection means;

• **Steps 3 and 4: act of response D, act of checking**

the controller device also comprises:

- means for the reception of the responses **D** coming from the demonstrator device, through the connection means,

- computation means, hereinafter called the computation means of the controller device, having **m** public values $G_1, G_2, \ldots, G_m$, to firstly compute a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$R' \equiv G_1{}^{d1} . G_2{}^{d2} . \ldots G_m{}^{dm} . D^v \bmod n$$

or a relationship of the type

$$R' \equiv D^v / G_1{}^{d1} . G_2{}^{d2} . \ldots G_m{}^{dm} . \bmod n$$

then, secondly, compute a token **T'** by applying the hashing function **h** having as arguments the message **M** and all or part of each reconstructed commitment **R'**,
the controller device also comprises:

- comparison means, hereinafter called the comparison means of the controller device, to compare the computed token **T'** with the received token **T**.

18. Controller device according to claim 15, designed to prove the authenticity of the message **M** by checking a signed message by means of an entity called a controller;
the signed message, sent by a signing device associated with a signing entity having a hashing function **h (message, R),** comprising:

- the message **M**,
- the challenges **d** and/or the commitments **R**,
- the responses **D**;

Checking operation

said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to a signing device associated with the signing entity,
said controller device having received the signed message from the signed device, through the connection means,
the controller device comprises:

- computation means, hereinafter called the computation means of the controller device,

- comparison means, hereinafter called the comparison means of the controller device;

• case where the controller device has commitments R, challenges d, responses D

if the controller has commitments **R**, challenges **d**, responses **D**,

• • the computation and comparison means of the controller device ascertain that the commitments **R**, the challenges **d** and the responses **D** satisfy relationships of the type

$$\mathbf{R \equiv G_1^{\ d1} . G_2^{\ d2} . \ldots G_m^{\ dm} . D^v \bmod n}$$

or relationships of the type:

$$\mathbf{R \equiv D^v / G_1^{\ d1} . G_2^{\ d2} . \ldots G_m^{\ dm} . \bmod n}$$

• • the computation and comparison means of the controller device ascertain that the message **M**, the challenges **d** and the commitments **R** satisfy the hashing function

$$\mathbf{d = h\ (message, R)}$$

• case where the controller device has challenges d and responses D

if the controller device has challenges **d** and responses **D**,

• • the computation means of the controller, on the basis of each challenge **d** and each response **D**, compute commitments **R'** satisfying relationships of the type

$$\mathbf{R' \equiv G_1^{\ d1} . G_2^{\ d2} . \ldots G_m^{\ dm} . D^v \bmod n}$$

or relationships of the type:

$$\mathbf{R' \equiv D^v / G_1^{\ d1} . G_2^{\ d2} . \ldots G_m^{\ dm} . \bmod n}$$

• • the computation and comparison means of the controller device ascertain that the message **M** and the challenges **d** satisfy the hashing function:

$$\mathbf{d = h\ (message, R')}$$

• case where the controller device has commitments R and responses D

if the controller device has commitments **R** and responses **D**,

• • the computation means of the controller device apply the hashing function and compute **d'** such that

$$d' = h\ (\text{message}, R)$$

• • the computation and comparison means of the controller device ascertain that the commitments **R,** the challenges **d'** and the responses **D** satisfy relationships of the type

$$R \equiv G_1^{\ d'1} . G_2^{\ d'2} . \ldots G_m^{\ d'm} . D^v \bmod n$$

or relationships of the type:

$$R \equiv D^v / G_1^{\ d'1} . G_2^{\ d'2} . \ldots G_m^{\ d'm} . \bmod n$$

09/889918

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
3 août 2000 (03.08.2000)

PCT

(10) Numéro de publication internationale
WO 00/45550 A3

(51) Classification internationale des brevets[7] : H04L 9/32

(21) Numéro de la demande internationale : PCT/FR00/00190

(22) Date de dépôt international : 27 janvier 2000 (27.01.2000)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
99/01065 27 janvier 1999 (27.01.1999) FR
99/03770 23 mars 1999 (23.03.1999) FR
99/12465 1 octobre 1999 (01.10.1999) FR
99/12467 1 octobre 1999 (01.10.1999) FR
99/12468 1 octobre 1999 (01.10.1999) FR

(71) Déposants *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR). **TELEDIFFUSION DE FRANCE** [FR/FR]; 10, rue d'Oradour-sur-Glane, F-75732 Paris cedex 15 (FR). **MATH RIZK** [BE/BE]; Verte Voie, 20 Boîte 5, B-1348 Louvain-la-Neuve (BE).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(pour US seulement)* : **GUILLOU, Louis** [FR/FR]; 16, rue de l'Ise, F-35230 Bourgbarre (FR). **QUISQUATER, Jean-Jacques** [BE/BE]; 3, avenue des Canards, B-1640 Rhode Saint Genese (BE).

(74) Mandataire : **VIDON, Patrice**; Cabinet Patrice Vidon, Immeuble Germanium, 80, avenue des Buttes de Coesmes, F-35700 Rennes (FR).

(81) États désignés *(national)* : AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée :
— *avec rapport de recherche internationale*

(88) Date de publication du rapport de recherche internationale: 25 avril 2002

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) Title: METHOD FOR PROVING THE AUTHENTICITY OR INTEGRITY OF A MESSAGE BY MEANS OF A PUBLIC EXPONENT EQUAL TO THE POWER OF TWO

(54) Titre : PROCEDE DESTINE A PROUVER L'AUTHENTICITE D'UNE ENTITE OU L'INTEGRITE D'UN MESSAGE AU MOYEN D'UN EXPOSANT PUBLIC EGAL A UNE PUISSANCE DE DEUX

(57) Abstract: Proof is established by means of the following parameters: m pairs of private values Q_i and public values G_i, m>1, a public module n made of the product of f first factors p_j, f>2, a public exponent v, linked to each other by relations of the type: $G_i.Q_i^v = 1 \bmod n$ or $G_i = Q_i^v \bmod n$. Said exponent v is such that $v=2^k$ where k>1 is a security parameter. Public value G_i is the square g_i^2 of a base number g_i that is lower than f first factors p_j, so that the two equations: $x2=g_i \bmod n$ and $x^2= -g_i \bmod n$ do not have a solution in x in the ring of the modulo n integers and such that the equation $x^v=g_i^2 \bmod n$ has solutions in x in the ring of the modulus n integers.

(57) Abrégé : La preuve est établie au moyen des paramètres suivants: m couples de valeurs privées Q_i et publiques G_i, m>1; un module public n constitué par le produit de f facteurs premiers p_j, f>2, un exposant public v, liés par des relations du type: $G_i.Q_i^v = 1 \bmod n$ ou $G_i=Q_i^v \bmod n$. Ledit exposant v est tel que $v = 2^k$ où k>1 est un paramètre de sécurité. Ladite valeur publique G_i est le carré g_i^2 d'un nombre de base g_i inférieur aux f facteurs premiers p_j, tel que les deux équations: $x^2 = g_i \bmod n$ et $x^2 = -g_i \bmod n$ n'ont pas de solution en x dans l'anneau des entiers modulo n, et tel que l'équation $x^v = g_i^2 \bmod n$ a des solutions en x dans l'anneau des entiers modulo n.

WO 00/45550 A3

Attorney Docket No. 9320 134USWO

MERCHANT & GOULD P.C.

United States Patent Application

COMBINED DECLARATION AND POWER OF ATTORNEY

As a below named inventor I hereby declare that: my residence, post office address and citizenship are as stated below next to my name; that

I verily believe I am the original, first and sole inventor (if only one name is listed below) or a joint inventor (if plural inventors are named below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: METHOD FOR PROVING THE AUTHENTICITY OF AN ENTITY AND/OR THE INTEGRITY OF A MESSAGE BY MEANS OF A PUBLIC EXPONENT EQUAL TO THE POWER OF TWO

The specification of which

(a. ☐ is attached hereto

b. ☒ was filed on as application serial no. and was amended on (if applicable) (in the case of a PCT-filed application) described and claimed in international no. PCT/FR00/00190 filed January 27, 2000 and as amended on January 10, 2001 (if any), which I have reviewed and for which I solicit a United States patent.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119/365 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on the basis of which priority is claimed:

a. ☐ no such applications have been filed.

b. ☒ such applications have been filed as follows:

FOREIGN APPLICATION(S), IF ANY, CLAIMING PRIORITY UNDER 35 USC § 119			
COUNTRY	**APPLICATION NUMBER**	**DATE OF FILING (day, month, year)**	**DATE OF ISSUE (day, month, year)**
France	99 01065	27 January 1999	
France	99 03770	23 March 1999	
France	99 12465	1 October 1999	
France	99 12467	1 October 1999	
France	99 12468	1 October 1999	
ALL FOREIGN APPLICATION(S), IF ANY, FILED BEFORE THE PRIORITY APPLICATION(S)			
COUNTRY	**APPLICATION NUMBER**	**DATE OF FILING (day, month, year)**	**DATE OF ISSUE (day, month, year)**

I hereby claim the benefit under Title 35, United States Code, § 120/365 of any United States and PCT international application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, § 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application.

U.S. APPLICATION NUMBER	DATE OF FILING (day, month, year)	STATUS (patented, pending, abandoned)

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below:

U.S. PROVISIONAL APPLICATION NUMBER	DATE OF FILING (Day, Month, Year)

I acknowledge the duty to disclose information that is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, § 1.56 (reprinted below):

§ 1.56 Duty to disclose information material to patentability.

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclose information exists with respect to each pending claim until the claim is canceled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is canceled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§ 1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

(1) prior art cited in search reports of a foreign patent office in a counterpart application, and

(2) the closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made of record in the application, and

(1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim;

or

(2) It refutes, or is inconsistent with, a position the applicant takes in:

(i) Opposing an argument of unpatentability relied on by the Office, or

(ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

(1) Each inventor named in the application:

(2) Each attorney or agent who prepares or prosecutes the application; and

(3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.

(e) In any continuation-in-part application, the duty under this section includes the duty to disclose to the Office all information known to the person to be material to patentability, as defined in paragraph (b) of this section, which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby appoint the following attorney(s) and/or patent agent(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith:

Albrecht, John W.	Reg. No. 40,481
Ali, M. Jeffer	Reg. No. 46,359
Altera, Allan G	REg No 40,274
Anderson, Gregg I.	Reg. No. 28,828
Batzli, Brian H.	Reg. No. 32,960
Beard, John L.	Reg. No. 27,612
Berns, John M.	Reg. No. 43,496
Branch, John W.	Reg. No. 41,633
Bremer, Dennis C.	Reg. No. 40,528
Brown, Jeffrey C.	Reg. No. 41,643
Bruess, Steven C.	Reg No. 34,130
Byrne, Linda M.	Reg. No. 32,404
Campbell, Keith	Reg. No. 46,597
Carlson, Alan G.	Reg. No. 25,959
Caspers, Philip P.	Reg. No. 33,227
Clifford, John A.	Reg. No. 30,247
Coldren, Richard J	Reg. No 44,084
Daignault, Ronald A.	Reg. No. 25,968
Daley, Dennis R.	Reg. No. 34,994
Dalglish, Leslie E.	Reg. No. 40,579
Daulton, Julie R.	Reg. No. 36,414
DeVries Smith, Katherine M.	Reg. No. 42,157
DiPietro, Mark J.	Reg. No. 28,707
Doscotch, Matthew A.	Reg No. P48,957
Edell, Robert T.	Reg. No. 20,187
Epp Ryan, Sandra	Reg No. 39,667
Glance, Robert J	Reg. No. 40,620
Goggin, Matthew J.	Reg. No. 44,125
Golla, Charles E.	Reg. No. 26,896
Gorman, Alan G.	Reg. No. 38,472
Gould, John D.	Reg. No. 18,223
Gregson, Richard	Reg. No. 41,804
Gresens, John J.	Reg. No. 33,112
Hamer, Samuel A.	Reg. No. 46,754
Hamre, Curtis B.	Reg. No. 29,165
Harrison, Kevin C.	Reg. No. 46,759
Hertzberg, Brett A.	Reg. No. 42,660
Hillson, Randall A.	Reg. No. 31,838
Holzer, Jr., Richard J.	Reg. No. 42,668
Hope, Leonard J.	Reg. No. 44,774
Jardine, John S.	Reg. No. P-48,835
Johnston, Scott W.	Reg. No. 39,721
Kadievitch, Natalie D.	Reg. No. 34,196
Kaseburg, Frederick A.	Reg. No. 47,695
Kettelberger, Denise	Reg. No. 33,924
Keys, Jeramie J.	Reg. No. 42,724
Knearl, Homer L.	Reg. No. 21,197
Kowalchyk, Alan W.	Reg. No. 31,535
Kowalchyk, Katherine M.	Reg. No. 36,848
Lacy, Paul E.	Reg. No 38,946
Larson, James A.	Reg. No. 40,443
Leon, Andrew J.	Reg. No. 46,869
Leonard, Christopher J	Reg. No 41,940
Liepa, Mara E.	Reg. No. 40,066
Lindquist, Timothy A.	Reg. No. 40,701
Lown, Jean A.	Reg. No. P48,428
Mayfield, Denise L.	Reg. No. 33,732
McDonald, Daniel W.	Reg. No. 32,044
McIntyre, Jr., William F.	Reg. No. 44,921
Mitchem, M. Todd	Reg. No. 40,731
Mueller, Douglas P.	Reg. No 30,300
Nelson, Anna	Reg No. P48,935
Parsons, Nancy J.	Reg. No. 40,364
Pauly, Daniel M.	Reg. No. 40,123
Phillips, John B.	Reg. No. 37,206
Pino, Mark J.	Reg. No. 43,858
Prendergast, Paul	Reg. No. 46,068
Pytel, Melissa J.	Reg. No. 41,512
Qualey, Terry	Reg. No. 25,148
Reich, John C.	Reg. No. 37,703
Reiland, Earl D.	Reg. No. 25,767
Roberts, Fred	Reg. No. 34,707
Samuels, Lisa A.	Reg. No. 43,080
Schmaltz, David G.	Reg. No. 39,828
Schuman, Mark D.	Reg. No. 31,197
Schumann, Michael D.	Reg. No. 30,422
Scull, Timothy B.	Reg. No. 42,137
Sebald, Gregory A.	Reg. No. 33,280
Skoog, Mark T.	Reg. No. 40,178
Spellman, Steven J.	Reg. No. 45,124
Stoll-DeBell, Kirstin L.	Reg. No. 43,164
Sullivan, Timothy	Reg. No. 47,981
Sumner, John P.	Reg. No. 29,114
Swenson, Erik G.	Reg. No. 45,147
Tellekson, David K.	Reg. No. 32,314
Trembath, Jon R.	Reg. No. 38,344
Tunheim, Marcia A	Reg. No. 42,189
Underhill, Albert L.	Reg. No. 27,403
Vandenburgh, J. Derek	Reg. No 32,179
Wahl, John R.	Reg. No. 33,044
Weaver, Karrie G.	Reg. No. 43,245
Welter, Paul A.	Reg. No. 20,890
Whipps, Brian	Reg. No. 43,261
Whitaker, John E.	Reg. No. 42,222
Williams, Douglas J.	Reg. No. 27,054
Withers, James D.	Reg. No. 40,376
Witt, Jonelle	Reg. No. 41,980
Wu, Tong	Reg. No. 43,361
Xu, Min S.	Reg. No. 39,536
Young, Thomas	Reg. No. 25,796
Zeuli, Anthony R.	Reg. No. 45,255

I hereby authorize them to act and rely on instructions from and communicate directly with the person/assignee/attorney/firm/ organization who/which first sends/sent this case to them and by whom/which I hereby declare that I have consented after full disclosure to be represented unless/until I instruct Merchant & Gould P.C. to the contrary.

I understand that the execution of this document, and the grant of a power of attorney, does not in itself establish an attorney-client relationship between the undersigned and the law firm Merchant & Gould P.C., or any of its attorneys.

Please direct all correspondence in this case to Merchant & Gould P.C. at the address indicated below:

Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903

23552
PATENT TRADEMARK OFFICE

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2	**Full Name Of Inventor**	**Family Name** Guillou	**First Given Name** Louis	**Second Given Name**
0	**Residence & Citizenship**	**City** Bourgbarre	**State or Foreign Country** France	**Country of Citizenship** France
1	**Mailing Address**	**Address** 16, rue de l'Ise	**City** Bourgbarre	**State & Zip Code/Country** 35230 / France
Signature of Inventor 201:	L GUILLOU		**Date:** 16 août 2001	
2	**Full Name Of Inventor**	**Family Name** Quisquater	**First Given Name** Jean-Jacques	**Second Given Name**
0	**Residence & Citizenship**	**City** Rhode Saint Genese	**State or Foreign Country** Belgium	**Country of Citizenship** Belgium
2	**Mailing Address**	**Address** 3, avenue des Canards	**City** Rhode Saint Genese	**State & Zip Code/Country** 1640 / Belgium
Signature of Inventor 202:	J.J. [illegible]		**Date:** 20 août 2001	